(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6149749号
(P6149749)

(45)発行日　平成29年6月21日(2017.6.21)　(24)登録日　平成29年6月2日(2017.6.2)

(51)Int.Cl.		F I		
G06F 21/60	(2013.01)	G06F	21/60	320
G06F 12/00	(2006.01)	G06F	12/00	545A
		G06F	12/00	537H

請求項の数 12　(全 17 頁)

(21)出願番号　特願2014-20756(P2014-20756)
(22)出願日　平成26年2月5日(2014.2.5)
(65)公開番号　特開2015-148902(P2015-148902A)
(43)公開日　平成27年8月20日(2015.8.20)
審査請求日　平成28年3月9日(2016.3.9)

(73)特許権者　000005496
富士ゼロックス株式会社
東京都港区赤坂九丁目７番３号
(74)代理人　110000154
特許業務法人はるか国際特許事務所
(72)発明者　猪股　浩司郎
神奈川県横浜市西区みなとみらい六丁目１番　富士ゼロックス株式会社内

審査官　岸野　徹

最終頁に続く

(54)【発明の名称】情報処理装置、情報処理システム、及びプログラム

(57)【特許請求の範囲】

【請求項１】

利用者の指示に基づいてファイルを取得するファイル取得手段と、

前記ファイル取得手段により取得された前記ファイルを暗号化するとともに、前記暗号化されたファイルを復号するための暗号鍵を生成する生成手段と、

前記生成手段により生成された前記暗号鍵により、前記ファイル取得手段により取得された前記ファイルを暗号化するとともに、前記暗号化されたファイルを、前記利用者が所持する利用者端末とは異なるファイルサーバに保存するデータ処理手段と、

前記生成手段により生成された前記暗号鍵を取得するための情報を紙媒体に印刷する出力手段と、

前記暗号化されたファイルの所在を示す所在情報を、前記利用者端末に送信する送信手段と、

を含み、

前記暗号鍵を取得するための情報と、前記所在情報とは、別々に出力される、

ことを特徴とする情報処理装置。

【請求項２】

利用者の指示に基づいて、該利用者を識別する利用者識別情報を取得する利用者識別情報取得手段と、

前記利用者識別情報と前記利用者端末の端末情報とを関連付けて記憶する利用者情報記憶手段から、前記利用者識別情報取得手段により取得された前記利用者識別情報に関連付

けられた前記端末情報を取得する端末情報取得手段と、を更に含み、
前記送信手段は、前記端末情報取得手段により取得された前記端末情報に基づく前記利用者端末に前記所在情報を送信する、
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】
前記暗号鍵を符号化する制限情報符号化手段を更に含み、
前記出力手段は、前記制限情報符号化手段により符号化された前記暗号鍵を前記紙媒体に印刷する、
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４】
前記暗号鍵を文字列化する制限情報文字列化手段を更に含み、
前記制限情報符号化手段は、前記制限情報文字列化手段により文字列化された前記暗号鍵を符号化する、ことを特徴とする請求項３に記載の情報処理装置。
【請求項５】
前記暗号鍵を分割する制限情報分割手段を更に含み、
前記符号化手段は、前記制限情報分割手段により分割された前記暗号鍵を符号化する、
ことを特徴とする請求項３に記載の情報処理装置。
【請求項６】
前記暗号鍵を分割する制限情報分割手段を更に含み、
前記制限情報文字列化手段は、前記制限情報分割手段により分割された前記暗号鍵を文字列化する、
ことを特徴とする請求項４に記載の情報処理装置。
【請求項７】
前記制限情報文字列化手段は、更に、前記暗号鍵とは別の制限情報であるダミー制限情報を文字列化し、
前記制限情報符号化手段は、更に、前記制限情報文字列化手段により文字列化された前記ダミー制限情報を符号化し、
前記出力手段は、更に、前記制限情報符号化手段により符号化された前記ダミー制限情報を取得するための情報を前記紙媒体に印刷する、
ことを特徴とする請求項４に記載の情報処理装置。
【請求項８】
前記ダミー制限情報は、前記暗号鍵とは別の暗号鍵であるダミー暗号鍵である、
ことを特徴とする請求項７に記載の情報処理装置。
【請求項９】
前記暗号鍵及び前記ダミー暗号鍵を分割する制限情報分割手段を更に含み、
前記制限情報文字列化手段は、前記制限情報分割手段により分割された前記暗号鍵及び前記ダミー暗号鍵を文字列化する、
ことを特徴とする請求項８に記載の情報処理装置。
【請求項１０】
利用者が利用する情報処理装置と、該情報処理装置にネットワークを介して接続された、該利用者が所持する利用者端末と、を含む情報処理システムであって、
前記情報処理装置は、
前記利用者の指示に基づいてファイルを取得する第１ファイル取得手段と、
前記第１ファイル取得手段により取得された前記ファイルを暗号化するとともに、前記暗号化されたファイルを復号するための暗号鍵を生成する生成手段と、
前記生成手段により生成された前記暗号鍵により、前記第１ファイル取得手段により取得された前記ファイルを暗号化するとともに、前記暗号化されたファイルを、前記利用者が所持する利用者端末とは異なるファイルサーバに保存するデータ処理手段と、
前記生成手段により生成された前記暗号鍵を取得するための情報を紙媒体に印刷する出力手段と、

前記暗号化されたファイルの所在を示す所在情報を、前記利用者端末に送信する送信手段と、
を含み、
前記利用者端末は、
前記紙媒体に印刷された前記暗号鍵を取得するための情報から前記暗号鍵を復元する制限情報取得手段と、
前記送信手段から送信された前記所在情報を取得する所在情報取得手段と、
前記所在情報取得手段により取得された前記所在情報に基づいて、前記ファイルサーバに保存された、前記暗号化されたファイルを取得する第２ファイル取得手段と、
前記制限情報取得手段により復元された前記暗号鍵により、前記第２ファイル取得手段により取得された前記暗号化されたファイルを復号する制限解除手段と、
を含み、
前記暗号鍵を取得するための情報と、前記所在情報とは、別々に出力される、
ことを特徴とする情報処理システム。
【請求項１１】
前記制限情報取得手段は、前記利用者端末が備える撮像手段により、前記暗号鍵を取得するための情報を撮像して、前記暗号鍵を復元する、
ことを特徴とする請求項１０に記載の情報処理システム。
【請求項１２】
利用者の指示に基づいてファイルを取得するファイル取得手段、
前記ファイル取得手段により取得された前記ファイルを暗号化するとともに、前記暗号化されたファイルを復号するための暗号鍵を生成する生成手段、
前記生成手段により生成された前記暗号鍵により、前記ファイル取得手段により取得された前記ファイルを暗号化するとともに、前記暗号化されたファイルを、前記利用者が所持する利用者端末とは異なるファイルサーバに保存するデータ処理手段、
前記生成手段により生成された前記暗号鍵を取得するための情報を紙媒体に印刷する出力手段、及び、
前記暗号化されたファイルの所在を示す所在情報を、前記利用者端末に送信する送信手段と、
としてコンピュータを機能させるためのプログラムであって、
前記暗号鍵を取得するための情報と、前記所在情報とは、別々に出力される、プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置、情報処理システム、及びプログラムに関する。
【背景技術】
【０００２】
近年、情報機器の紛失や情報機器のコンピュータウィルス等のマルウェアによる被害により、データの漏洩が問題となっている。
【０００３】
下記特許文献１には、ＣＣＤカメラで撮影した小物の画像データと、データベースに登録されている画像データとを照合してコンピュータシステムへのログインの判定を行うログイン方式に関する技術が開示されている。
【０００４】
下記特許文献２には、表示端末に表示された、公開暗号鍵を使って暗号化された後に２次元符号化された電子メールを、秘密暗号鍵を有する携帯端末で撮影することで復号する電子メール処理システムに関する技術が開示されている。
【先行技術文献】
【特許文献】

【０００５】
【特許文献１】特開平１１－０９６１２０号公報
【特許文献２】特開２００８－０５２５３７号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
本発明の目的は、データの漏洩を防止することができる情報処理装置を提供することである。
【課題を解決するための手段】
【０００７】
請求項１に記載の情報処理装置は、利用者の指示に基づいてファイルを取得するファイル取得手段と、前記ファイル取得手段により取得された前記ファイルへのアクセスを制限する制限情報を生成する生成手段と、前記生成手段により生成された前記制限情報を、前記ファイル取得手段により取得された前記ファイルに関連付けるデータ処理手段と、前記生成手段により生成された前記制限情報を紙媒体に出力する出力手段と、を含むことを特徴とする。
【０００８】
請求項２に記載の情報処理装置は、請求項１に記載の情報処理装置において、前記制限情報は、暗号鍵であり、前記データ処理手段は、前記ファイル取得手段により取得された前記ファイルを前記暗号鍵により暗号化する、ことを特徴とする。
【０００９】
請求項３に記載の情報処理装置は、請求項１又は２に記載の情報処理装置において、前記データ処理手段は、更に、前記制限情報が関連付けられた前記ファイルをファイル記憶手段に記憶し、前記制限情報が関連付けられた前記ファイルの所在を示す所在情報を、前記利用者が所持する利用者端末に送信する送信手段を更に含む、ことを特徴とする。
【００１０】
請求項４に記載の情報処理装置は、請求項３に記載の情報処理装置において、利用者の指示に基づいて、該利用者を識別する利用者識別情報を取得する利用者識別情報取得手段と、前記利用者識別情報と前記利用者が所持する利用者端末の端末情報とを関連付けて記憶する利用者情報記憶手段から、前記利用者識別情報取得手段により取得された前記利用者識別情報に関連付けられた前記端末情報を取得する端末情報取得手段と、を更に含み、前記送信手段は、前記端末情報取得手段により取得された前記端末情報に基づく前記利用者端末に前記所在情報を送信する、ことを特徴とする。
【００１１】
請求項５に記載の情報処理装置は、請求項３に記載の情報処理装置において、利用者の指示に基づいて、該利用者を識別する利用者識別情報を取得する利用者識別情報取得手段と、前記利用者識別情報と前記利用者が所持する利用者端末の端末情報とを関連付けて記憶する利用者情報記憶手段から、前記利用者識別情報取得手段により取得された前記利用者識別情報に関連付けられた前記端末情報を取得する端末情報取得手段と、を更に含み、前記送信手段は、前記端末情報取得手段により取得された前記端末情報に基づく前記利用者端末に前記制限情報が関連付けられた前記ファイルを送信する、ことを特徴とする。
【００１２】
請求項６に記載の情報処理装置は、請求項２に記載の情報処理装置において、前記暗号鍵を符号化する制限情報符号化手段を更に含み、前記出力手段は、前記制限情報符号化手段により符号化された前記暗号鍵を前記紙媒体に出力する、ことを特徴とする。
【００１３】
請求項７に記載の情報処理装置は、請求項６に記載の情報処理装置において、前記暗号鍵を文字列化する制限情報文字列化手段を更に含み、前記制限情報符号化手段は、前記制限情報文字列化手段により文字列化された前記暗号鍵を符号化する、ことを特徴とする。
【００１４】

請求項８に記載の情報処理装置は、請求項６に記載の情報処理装置において、前記暗号鍵を分割する制限情報分割手段を更に含み、前記符号化手段は、前記制限情報分割手段により分割された前記暗号鍵を符号化する、ことを特徴とする。

【００１５】

請求項９に記載の情報処理装置は、請求項７に記載の情報処理装置において、前記暗号鍵を分割する制限情報分割手段を更に含み、前記制限情報文字列化手段は、前記制限情報分割手段により分割された前記暗号鍵を文字列化する、ことを特徴とする。

【００１６】

請求項１０に記載の情報処理装置は、請求項７に記載の情報処理装置において、記制限情報文字列化手段は、更に、前記暗号鍵とは別の制限情報であるダミー制限情報を文字列化し、前記制限情報符号化手段は、更に、前記制限情報文字列化手段により文字列化された前記ダミー制限情報を符号化し、前記出力手段は、更に、前記制限情報符号化手段により符号化された前記ダミー制限情報を前記紙媒体に出力する、ことを特徴とする。

【００１７】

請求項１１に記載の情報処理装置は、請求項１０に記載の情報処理装置において、前記ダミー制限情報は、前記暗号鍵とは別の暗号鍵であるダミー暗号鍵である、ことを特徴とする。

【００１８】

請求項１２に記載の情報処理装置は、請求項１１に記載の情報処理装置において、前記暗号鍵及び前記ダミー暗号鍵を分割する制限情報分割手段を更に含み、前記制限情報文字列化手段は、前記制限情報分割手段により分割された前記暗号鍵及び前記ダミー暗号鍵を文字列化する、ことを特徴とする。

【００１９】

請求項１３に記載の情報処理システムは、利用者が利用する情報処理装置と、該情報処理装置にネットワークを介して接続された、該利用者が所持する利用者端末と、を含む情報処理システムであって、前記情報処理装置は、前記利用者の指示に基づいてファイルを取得する第１ファイル取得手段と、前記第１ファイル取得手段により取得された前記ファイルへのアクセスを制限する制限情報を生成する生成手段と、前記生成手段により生成された前記制限情報を、前記第１ファイル取得手段により取得された前記ファイルに関連付けると共に、前記制限情報が関連付けられた前記ファイルをファイル記憶手段に記憶するデータ処理手段と、前記生成手段により生成された前記制限情報を、紙媒体に出力する出力手段と、前記制限情報が関連付けられた前記ファイルの所在を示す所在情報を、前記利用者が所持する利用者端末に送信する送信手段と、を含み、前記利用者端末は、前記紙媒体に出力された前記制限情報を取得する制限情報取得手段と、前記送信手段から送信された前記所在情報を取得する所在情報取得手段と、前記所在情報取得手段により取得された前記所在情報に基づいて、前記制限情報が関連付けられた前記ファイルを取得する第２ファイル取得手段と、前記制限情報取得手段により取得された前記制限情報に基づいて、前記第２ファイル取得手段により取得された前記ファイルへのアクセスの制限を解除する制限解除手段と、を含む、ことを特徴とする。

【００２０】

請求項１４に記載の情報処理システムは、請求項１３に記載の情報処理システムにおいて、前記制限情報は、暗号鍵であり、前記データ処理手段は、前記第１ファイル取得手段により取得された前記ファイルを前記暗号鍵により暗号化し、前記制限解除手段は、前記制限情報取得手段により取得された前記暗号鍵により、前記第２ファイル取得手段により取得された前記ファイルを復号する、ことを特徴とする。

【００２１】

請求項１５に記載の情報処理システムは、請求項１４に記載の情報処理システムにおいて、前記制限情報取得手段は、前記利用者端末が備える撮像手段により前記制限情報を撮像して前記制限情報を取得する、ことを特徴とする。

【００２２】

請求項１６に記載のプログラムは、利用者の指示に基づいてファイルを取得するファイル取得手段、前記ファイル取得手段により取得された前記ファイルへのアクセスを制限する制限情報を生成する生成手段、前記生成手段により生成された前記制限情報を、前記ファイル取得手段により取得された前記ファイルに関連付けるデータ処理手段、及び、前記生成手段により生成された前記制限情報を紙媒体に出力する出力手段、としてコンピュータを機能させる。

【発明の効果】

【００２３】

請求項１、１３、１４、１５、及び１６に記載の発明によれば、ファイルへのアクセスを制限する制限情報を電子データではない形態として出力することができる。

【００２４】

請求項２に記載の発明によれば、暗号鍵によりファイルを暗号化することができる。

【００２５】

請求項３に記載の発明によれば、アクセスの制限の処理がされたファイルの所在を示す情報を利用者端末に送信することができる。

【００２６】

請求項４に記載の発明によれば、利用者を識別する情報を取得して、当該利用者を識別する情報に関連付けられた利用者端末に、アクセスの制限の処理がされたファイルの所在を示す情報を送信することができる。

【００２７】

請求項５に記載の発明によれば、利用者を識別する情報を取得して、当該利用者を識別する情報に関連付けられた利用者端末に、アクセスの制限の処理がされたファイルを送信することができる。

【００２８】

請求項６に記載の発明によれば、暗号鍵を符号化して紙媒体に出力することができる。

【００２９】

請求項７に記載の発明によれば、暗号鍵を文字列化及び符号化して紙媒体に出力することができる。

【００３０】

請求項８及び９に記載の発明によれば、暗号鍵を複数の部分に分割して紙媒体に出力することができる。

【００３１】

請求項１０乃至１２に記載の発明によれば、ファイルのアクセスの制限の処理に用いたものとは別の暗号鍵であるダミー鍵を紙媒体に出力することができる。

【図面の簡単な説明】

【００３２】

【図１】本発明に係る情報処理システムのハードウェア構成の一例を示す図である。

【図２】情報処理装置により実現される機能の一例を示す図である。

【図３】紙媒体に出力された暗号鍵の一例を示す図である。

【図４】利用者端末により実現される機能の一例を示す図である。

【図５】情報処理装置の処理のフローの一例を示す図である。

【図６】利用者端末の処理のフローの一例を示す図である。

【図７】情報処理装置により実現される機能の変形例を示す図である。

【図８】紙媒体に出力された暗号鍵の変形例を示す図である。

【発明を実施するための形態】

【００３３】

以下、本発明の実施形態について、図面を参照しつつ説明する。尚、図面については、同一または同等の要素には同一の符号を付し、重複する説明は省略する。

【００３４】

図１は、本実施形態に係る情報処理システムのハードウェア構成の概要について説明す

るための図である。情報処理システム１００は、情報処理装置１１０、利用者端末１２０、及びファイルサーバ１３０を含む。情報処理装置１１０、利用者端末１２０、及びファイルサーバ１３０は、それぞれインターネット等のネットワークに接続されている。

【００３５】

情報処理装置１１０は、制御部１１１、記憶部１１２、通信部１１３、及び印刷部１１４を含む。制御部１１１は、例えば、ＣＰＵ等であって、記憶部１１２に格納されたプログラムに従って動作し、情報処理装置１１０が行う各処理を実行する。記憶部１１２は、例えば、ＲＯＭやハードディスク等であり、制御部１１１によって実行されるプログラムを保持する。通信部１１３は、ネットワークインターフェイスであって、制御部１１１からの指示に応じて、ネットワークを介して情報を送受信する。印刷部１１４は、例えば、電子写真方式等により紙等の記録媒体に画像を形成する。尚、印刷部１１４は、情報処理装置１１０とは別の、直接又はネットワークを介して情報処理装置１１０に接続された装置に含まれていてもよい。

【００３６】

利用者端末１２０は、利用者が利用する情報端末であって、制御部１２１、記憶部１２２、通信部１２３、及び撮像部１２４を含む。制御部１２１は、例えば、ＣＰＵ等であって、記憶部１２２に格納されたプログラムに従って動作し、利用者端末１２０が行う各処理を実行する。記憶部１２２は、例えば、ＲＯＭやハードディスク等であり、制御部１２１によって実行されるプログラムを保持する。通信部１２３は、ネットワークインターフェイスであって、制御部１２１からの指示に応じて、ネットワークを介して情報を送受信する。撮像部１２４は、例えば、カメラ等であって、画像を取得する。

【００３７】

ファイルサーバ１３０（ファイル記憶手段）は、電子データを保存するもので、所謂クラウドサーバと呼ばれるデータサーバであってもよい。また、ファイルサーバ１３０は、情報処理装置１１０及び利用者端末１２０のいずれもがネットワークを介してアクセスできるデータサーバである。

【００３８】

尚、上記制御部１１１、１２１で処理されるプログラムは、例えば、光ディスク、磁気ディスク、磁気テープ、光磁気ディスク、フラッシュメモリ等のコンピュータ可読な情報記憶媒体を介して提供されてもよいし、又は、インターネット等の通信手段を介して提供されてもよい。

【００３９】

次に、情報処理装置１１０により実現される機能について説明する。図２は、情報処理装置１１０により実現される機能を説明するための図である。図２に示す通り、情報処理装置１１０は、機能的には、例えば、ファイル取得部２０１、データ処理部２０２、制限情報生成部２０３、制限情報文字列化部２０４、制限情報符号化部２０５、制限情報出力部２０６、利用者識別情報取得部２０７、端末情報取得部２０８、利用者情報記憶部２０９、及び所在情報送信部２１０を含む。

【００４０】

ファイル取得部２０１は、利用者の指示に基づいてファイルを取得する。ファイルは、情報処理装置１１０、又は情報処理装置１１０に直接或いはネットワークを介して接続されている情報機器に記憶されているものから取得されてもよいし、情報処理装置１１０、又は情報処理装置１１０に直接或いはネットワークを介して接続されている、例えば、スキャナ等の画像ファイル取得装置が取得したファイルから取得されてもよい。ファイル取得部２０１は、取得したファイルをデータ処理部２０２に渡す。

【００４１】

データ処理部２０２は、ファイル取得部２０１からファイルを取得すると、制限情報生成部２０３に、取得したファイルへのアクセスを制限する制限情報の生成を要求する。

【００４２】

制限情報生成部２０３は、データ処理部２０２から制限情報の生成要求を取得すると、

制限情報を生成する。なお、以下では、制限情報の一例として、ファイルを暗号化するための暗号鍵を挙げて説明する。具体的には、制限情報生成部２０３は、公知の乱数発生技術を用いて、ランダムな値から成る暗号鍵を生成する。暗号鍵としては、１２８ｂｉｔ以上の乱数列を生成するのが望ましい。暗号鍵は、所謂バイナリデータ形式の電子データである。制限情報生成部２０３は、生成した暗号鍵をデータ処理部２０２に渡す。

【００４３】

データ処理部２０２は、制限情報生成部２０３から取得した暗号鍵をファイル取得部２０１から取得したファイルに関連付ける。具体的には、データ処理部２０２は、制限情報生成部２０３により生成された暗号鍵により、ファイル取得部２０１から取得したファイルを暗号化する。暗号化には、公知のＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）等の方式を用いればよい。更に、データ処理部２０２は、暗号化されたファイルを、ネットワークを介して情報処理装置１１０に接続されたファイルサーバ１３０に保存し、暗号化されたファイルの所在を示す情報である所在情報をファイル名に関連付けて後述の所在情報送信部２１０に渡す。具体的には、データ処理部２０２は、暗号化されたファイルのファイル名と、ファイルサーバ１３０における、暗号化されたファイルが保存された場所を示すアドレス情報（例えば、ＵＲＬ）とを、所在情報送信部２１０に渡す。また、データ処理部２０２は、制限情報生成部２０３から取得した暗号鍵を、ファイル取得部２０１から取得したファイルのファイル名に関連付けて制限情報文字列化部２０４に渡す。

【００４４】

制限情報文字列化部２０４は、データ処理部２０２から取得した暗号鍵を文字列化する。具体的には、制限情報文字列化部２０４は、公知のＢａｓｅ６４　ｅｎｃｏｄｅ等の方式を用いて、データ処理部２０２から取得した暗号鍵を文字列化する。文字列化により、データ処理部２０２から取得したバイナリデータである暗号鍵は、所謂テキストデータに変換される。制限情報文字列化部２０４は、データ処理部２０２から取得した暗号鍵を文字列化し、文字列化された暗号鍵を制限情報符号化部２０５に渡す。

【００４５】

制限情報符号化部２０５は、制限情報文字列化部２０４から取得した文字列化された暗号鍵を符号化する。具体的には、制限情報符号化部２０５は、公知の技術を用いて、制限情報文字列化部２０４から取得した文字列化された暗号鍵を符号化する。本実施形態においては、制限情報符号化部２０５は、文字列化された暗号鍵を、例えばＱＲコード（登録商標）化する。尚、符号化については、視覚化された符号に変換されるものであれば特に限定されるものではなく、ＱＲコードに限らず、例えば、バーコードやＭＩＧ等に変換されてもよい。制限情報符号化部２０５は、制限情報文字列化部２０４から取得した文字列化された暗号鍵を符号化し、符号化された暗号鍵を制限情報出力部２０６に渡す。

【００４６】

制限情報出力部２０６は、制限情報符号化部２０５から取得した符号化された暗号鍵を紙媒体に出力する。具体的には、制限情報出力部２０６は、例えば、印刷部１１４に符号化された暗号鍵（ＱＲコード）の印刷を指示する。

【００４７】

図３は、紙媒体に出力された暗号鍵の一例を示す図である。図３に示す通り、符号化された暗号鍵３０２（ＱＲコード）が紙媒体３０１の上に印刷されている。印刷された紙媒体３０１は、情報処理装置１１０を操作する利用者が取得し保管する。

【００４８】

図２に戻り、更に、情報処理装置１１０により実現される機能について説明する。利用者識別情報取得部２０７は、利用者の指示に基づいて、当該利用者を識別する利用者識別情報を取得する。具体的には、利用者識別情報取得部２０７は、例えば、利用者が、情報処理装置１１０に接続されたＩＣタグ・チップ読み取り機に、利用者を識別する利用者識別情報が書き込まれたＩＣタグ・チップをかざした際に、利用者識別情報を取得する。ここで、利用者識別情報とは、予め利用者に付与された、利用者を一意に識別する情報（例

えば、ＩＤ番号）である。尚、利用者識別情報の取得は、ＩＣタグ・チップを読み取る態様に限らず、利用者識別情報を符号化した符号（ＱＲコード、バーコード等）をコードリーダーにより読み取るようにしてもよいし、利用者が利用者識別情報を情報処理装置１１０に直接入力するようにしてもよい。利用者識別情報取得部２０７は、取得した利用者識別情報を端末情報取得部２０８に渡す。

【００４９】

端末情報取得部２０８は、利用者識別情報取得部２０７から取得した利用者識別情報に基づいて利用者端末１２０の端末情報を取得する。具体的には、端末情報取得部２０８は、利用者識別情報と端末情報とを関連付けて記憶する利用者情報記憶部２０９から、当該利用者識別情報に該当する利用者が所持する利用者端末１２０の端末情報を取得する。利用者情報記憶部２０９は、情報処理装置１１０に含まれていてもよいし、情報処理装置１１０の外部に設けられ、ネットワークを介して情報処理装置１１０に接続されていてもよい。ここで、端末情報とは、利用者端末１２０が利用可能なメールアドレス等の情報を含む。端末情報取得部２０８は、取得した端末情報を所在情報送信部２１０に渡す。

【００５０】

所在情報送信部２１０は、端末情報取得部２０８から取得した端末情報に基づいて、データ処理部２０２から取得した所在情報を利用者端末１２０に送信する。具体的には、所在情報送信部２１０は、端末情報に含まれた利用者端末１２０のメールアドレスに宛てて所在情報を送信する。送信されるメールには、例えば、件名に暗号化されたファイルのファイル名が含まれ、本文に暗号化されたファイルの保存先を示す所在情報が含まれる。

【００５１】

次に、利用者端末１２０により実現される機能について説明する。図４は、利用者端末１２０により実現される機能を説明するための図である。図４に示す通り、利用者端末１２０は、機能的には、例えば、制限情報取得部４０１、所在情報取得部４０２、端末側ファイル取得部４０３、及び制限解除部４０４を含む。

【００５２】

制限情報取得部４０１は、利用者の指示に基づいて、制限情報（ここでは、暗号鍵）を取得する。具体的には、利用者が利用者端末１２０に備えられた撮像部１２４により、情報処理装置１１０から出力された紙媒体３０１に印刷された符号化された暗号鍵３０２（ＱＲコード）を撮像すると、制限情報取得部４０１は、撮像された符号化された暗号鍵３０２から暗号鍵を復元する。具体的には、制限情報取得部４０１は、取得した符号化された暗号鍵３０２に、前述した情報処理装置１１０の制限情報符号化部２０５及び制限情報文字列化部２０４において行われた処理の復元処理を行うことによって暗号鍵を復元する。制限情報取得部４０１は、取得した暗号鍵を制限解除部４０４に渡す。

【００５３】

所在情報取得部４０２は、所在情報を取得する。具体的には、所在情報取得部４０２は、情報処理装置１１０の所在情報送信部２１０から送信された所在情報を、通信部１２３を介して取得する。所在情報取得部４０２は、取得した所在情報を端末側ファイル取得部４０３に渡す。

【００５４】

端末側ファイル取得部４０３は、所在情報取得部４０２から取得した所在情報に基づいて、暗号化されたファイルを取得する。具体的には、端末側ファイル取得部４０３は、所在情報に含まれている、暗号化されたファイルの保存先のアドレス情報（例えば、ＵＲＬ）を参照して、通信部１２３を介してファイルサーバ１３０にアクセスし、暗号化されたファイルを取得する。端末側ファイル取得部４０３は、取得した暗号化されたファイルを制限解除部４０４に渡す。

【００５５】

制限解除部４０４は、制限情報取得部４０１から取得した暗号鍵に基づいて、端末側ファイル取得部４０３から取得した暗号化されたファイルへのアクセスの制限を解除する。具体的には、制限解除部４０４は、制限情報取得部４０１から取得した暗号鍵により、端

末側ファイル取得部４０３から取得した暗号化されたファイルの復号を行う。暗号の復号には、情報処理装置１１０のデータ処理部２０２で行われた処理の復元処理が行われる。

【００５６】

次に、本実施形態における情報処理装置１１０の処理のフローの概要について説明する。図５は、情報処理装置１１０の処理のフローの一例を示す図である。図５は、情報処理装置１１０がファイルを取得してから、紙媒体３０１に符号化された暗号鍵３０２の出力を終了するまでの処理のフローを示す。

【００５７】

まず、ファイル取得部２０１がファイルを取得する（Ｓ５０１）。そして、制限情報生成部２０３が、暗号鍵を作成する（Ｓ５０２）。

【００５８】

次に、データ処理部２０２が、暗号鍵を用いてファイルを暗号化する（Ｓ５０３）。そして、データ処理部２０２は、暗号化されたファイルをファイルサーバ１３０に保存する（Ｓ５０４）。

【００５９】

次に、制限情報文字列化部２０４が、暗号鍵を文字列化する（Ｓ５０５）。そして、制限情報符号化部２０５が、文字列化された暗号鍵を符号化する（Ｓ５０６）。そして制限情報出力部２０６が、符号化された暗号鍵３０２（例えばＱＲコード）を紙媒体３０１に出力（印刷）する（Ｓ５０７）。

【００６０】

次に、利用者識別情報取得部２０７が、利用者の指示に基づいて利用者識別情報を取得し（Ｓ５０８）、端末情報取得部２０８が、利用者識別情報に関連付けられた端末情報を記憶する利用者情報記憶部２０９から端末情報を取得する（Ｓ５０９）。そして、所在情報送信部２１０が、端末情報に基づいて、暗号化されたファイルの所在を示す所在情報（例えばＵＲＬ）を送信する（Ｓ５１０）。所在情報を送信すると処理が終了される。

【００６１】

次に、本実施形態における利用者端末１２０の処理のフローの概要について説明する。図６は、利用者端末１２０の処理のフローの一例を示す図である。図６は、利用者端末１２０が符号化された暗号鍵３０２及び所在情報を取得してから、暗号化されたファイルの復号を終了するまでの処理のフローを示す。

【００６２】

まず、制限情報取得部４０１が、利用者の指示に基づいて取得された符号化された暗号鍵３０２（例えばＱＲコード）に、情報処理装置１１０の制限情報符号化部２０５及び制限情報文字列化部２０４において行われた処理のそれぞれの復元処理を行って、暗号鍵を取得する（Ｓ６０１）。そして、所在情報取得部４０２が、情報処理装置１１０の所在情報送信部２１０から送信された所在情報（例えばＵＲＬ）を取得する（Ｓ６０２）。

【００６３】

次に、端末側ファイル取得部４０３が、所在情報に基づいて、暗号化されたファイルが保存されたファイルサーバ１３０にアクセスし、暗号化されたファイルを取得する（Ｓ６０３）。そして、制限解除部４０４が、暗号化されたファイルを暗号鍵により復号する（Ｓ６０４）。暗号化されたファイルが復号されると処理が終了される。

【００６４】

本実施形態に係る情報処理装置１１０によれば、ファイルを暗号化するための暗号鍵が紙媒体３０１に電子データではない形態として出力される。よって、電子データでない暗号鍵は、電子データである暗号化されたファイルと隔離される。これにより、例えば、暗号化された電子データ（ファイル）が第三者に渡ったとしても、復号するための情報が印刷された紙媒体３０１が第三者に渡らない限り、ファイルの情報が漏えいすることはない。よって、暗号鍵を電子データとして保存（管理）する場合に比べて、データの漏洩が防止される。

【００６５】

[変形例]
上記実施形態では、ファイルの暗号化に用いられた暗号鍵を文字列化及び符号化したものを紙媒体３０１に出力する場合について説明した。本変形例では、ファイルを暗号化するための暗号鍵とは別（偽）の暗号鍵であるダミー鍵を更に生成し、更に、ダミー鍵を含む暗号鍵を分割、文字列化、及び符号化したものを紙媒体３０１に出力する場合について説明する。尚、本変形例においても、上記実施形態と同様に、制限情報は暗号鍵であるとする。また、説明の重複を避けるため、本変形例の説明においては、上記実施形態と異なる部分について主に説明する。

【００６６】
図７は、本変形例における情報処理装置１１０の機能を説明するための図である。図２に示した、上記実施形態における情報処理装置１１０の機能と異なる部分は主に以下の通りである。

【００６７】
制限情報生成部２０３は、データ処理部２０２から暗号鍵の生成要求を取得すると、ファイルを暗号化するための１つの暗号鍵と、ファイルを暗号化するためには用いられない、即ちファイルの暗号化とは無関係の暗号鍵である２つのダミー鍵を生成し、生成したすべての暗号鍵をデータ処理部２０２に渡す。

【００６８】
データ処理部２０２は、ファイルを暗号化するための暗号鍵を用いて、ファイル取得部から取得したファイルを暗号化し、すべての暗号鍵を制限情報分割部２１１に渡す。

【００６９】
制限情報分割部２１１は、データ処理部２０２から取得した暗号鍵を分割する。本変形例においては、制限情報分割部２１１は、データ処理部２０２から取得した３つの暗号鍵をそれぞれ、例えば３分割する。具体的には、制限情報分割部２１１は、各暗号鍵について、前半部、中間部、後半部に分割する。制限情報分割部２１１は、分割された暗号鍵のすべて（ここでは、９つの暗号鍵）を制限情報文字列化部２０４に渡す。

【００７０】
制限情報文字列化部２０４は、制限情報分割部から取得したすべての暗号鍵を文字列化する。そして、制限情報文字列化部２０４は、すべての文字列化された暗号鍵を制限情報符号化部２０５に渡す。

【００７１】
制限情報符号化部２０５は、制限情報文字列化部２０４から取得したすべての文字列化された暗号鍵を符号化する。本変形例においても、制限情報符号化部２０５は、文字列化された暗号鍵をＱＲコード化する。そして、制限情報符号化部２０５は、すべての符号化された暗号鍵を制限情報出力部２０６に渡す。

【００７２】
制限情報出力部２０６は、制限情報符号化部２０５から取得したすべての符号化された暗号鍵３０２を紙媒体３０１に出力する。具体的には、制限情報出力部２０６は、印刷部１１４にすべての符号化された暗号鍵３０２を配置したものの印刷を指示する。

【００７３】
図８は、本変形例における、紙媒体に出力された暗号鍵の一例を示す図である。図８に示す通り、９つの符号化された暗号鍵３０２（ＱＲコード）が１から９の番号を付されて紙媒体３０１に印刷されている。以上に述べた様に、これらの９つの符号化された暗号鍵３０２は、ファイルの暗号化に用いられた１つの暗号鍵と、ファイルの暗号化とは無関係な２つのダミー鍵をそれぞれ３分割したものから生成されたものである。即ち、これらの９つのＱＲコードのうち３つは、ファイルを暗号化する処理に使われた暗号鍵から生成されたものであり、残りの６つは、ファイルの暗号化とは無関係なダミー鍵から生成されたものである。例えば、図８において、番号「５」のＱＲコードがファイルの暗号化に用いられた１つの暗号鍵の前半部に対応し、番号「３」のＱＲコードが該暗号鍵の中間部に対応し、番号「９」のＱＲコードが該暗号鍵の後半部に対応している。印刷された紙媒体３

０１は、情報処理装置１１０を操作する利用者が取得し保管する。

【００７４】

ここで、上記９つのＱＲコードを配置する方法としては、種々の方法が考えられるが、例えば、情報処理装置１１０に備えられたタッチパネルや入力キー等のユーザーインターフェイスにより、利用者から指示を受け付ける方法が考えられる。この場合、例えば、利用者が、タッチパネルを操作して、ＱＲコードの配置を指定する情報として、配置位置に対応する「５」、「３」、「９」の番号を順に入力すると、最初に入力された番号「５」の位置にファイルの暗号化に用いられた暗号鍵の前半部に対応するＱＲコードが配置され、次に入力された番号「３」の位置に該暗号鍵の中間部に対応するＱＲコードが配置され、その次に入力された番号「９」の位置に該暗号鍵の後半部に対応するＱＲコードが配置され、入力されなかった、番号「１」、「２」、「４」、「６」、「７」、及び「８」の位置にファイルの暗号化とは無関係なダミー鍵から生成されたＱＲコードが配置されるようにすればよい。また、制限情報出力部２０６での紙媒体３０１への印刷は、ＱＲコードの配置の指定を受け付けた後に実行可能になるとしてもよい。

【００７５】

また、情報処理装置１１０において、ＱＲコードの配置位置と復元する際の順序とを自動的に決定する場合は、情報処理装置１１０が、決定した上記順序を示す順序情報を、利用者端末１２０に送信する構成としてもよい。なお、情報処理装置１１０は、ファイルの所在情報（例えばＵＲＬ）とともに、上記順序情報を送信してもよいし、上記所在情報とは別個に上記順序情報を送信してもよい。

【００７６】

次に、本変形例における、利用者端末１２０での暗号鍵の取得について説明する。上述の通り、紙媒体３０１には９つのＱＲコードが出力されているが、ファイルを暗号化する処理に使われた暗号鍵から生成されたものは、これらのうちの３つである。残りの６つは、ファイルを暗号化する処理に使われなかった、即ちダミー鍵から生成されたものである。よって、ＱＲコードの撮像に際しては、利用者は、９つのＱＲコードのうち、ファイルを暗号化する処理に使われた暗号鍵から生成された３つのＱＲコードを、復元のために必要な順序で撮像する必要がある。例えば、ファイルの暗号化に用いられた１つの暗号鍵が制限情報分割部２１１で分割されたときの前半部、中間部、後半部の順、即ち、図８において、前半部に対応する番号「５」のＱＲコード、中間部に対応する番号「３」のＱＲコード、後半部に対応する番号「９」のＱＲコードの順に撮像する必要がある。尚、利用者は、復元するための撮像順を、情報処理装置１１０の操作時（例えば、印刷指示の時）に取得（認識）することができる。

【００７７】

ＱＲコードが撮像されると、制限情報取得部４０１は、撮像されたＱＲコードから暗号鍵を復元する。具体的には、制限情報取得部４０１は、情報処理装置１１０の制限情報符号化部２０５、制限情報文字列化部２０４、及び制限情報分割部２１１において行われた処理の復元処理を行うことによって、暗号鍵を復元する。尚、ファイルを暗号化する処理に使われた暗号鍵から生成された３つのＱＲコードが、暗号鍵の復元のために必要な順序で撮像された以外の場合は、本処理において正しい暗号鍵が復元されない。暗号鍵が復元された後の処理については、上記実施形態と同様である。

【００７８】

本変形例によれば、ファイルの暗号化に用いられた暗号鍵と、ファイルの暗号化とは無関係のダミー鍵とが、それぞれ分割されて紙媒体３０１に出力される。これにより、例えば、暗号化された電子データ（ファイル）と、復号するための情報が印刷された紙媒体３０１とが、第三者に渡ったとしても、第三者が紙媒体３０１に印刷された情報（ＱＲコード）の撮像順を認識していない限り、ファイルの情報が漏えいすることはない。よって、更に、データの漏洩が防止される。

【００７９】

本発明は、上記実施の形態に限定されるものではなく、上記実施の形態で示した構成と

実質的に同一の構成、同一の作用効果を奏する構成又は同一の目的を達成することができる構成で置き換えてもよい。例えば、上記情報処理装置１１０及び利用者端末１２０の機能的構成や上記処理のフローは一例であって、本発明はこれに限定されるものではない。

【００８０】

例えば、暗号鍵はパスワードから生成されるとしてもよい。この場合、パスワードから暗号鍵の生成には、公知の手法を用い、例えば、パスワードを一方向ハッシュ関数（例えばｓｈａ２５６等）でハッシュ値をとり、それを暗号鍵とすればよい。また、制限情報は、暗号鍵に限定されず、パスワードであってもよい。制限情報がパスワードの場合、データ処理部２０２は、制限情報をファイルに関連付ける処理として、パスワードによりファイルを保護する処理をするようにしてもよい。また、上記のパスワードは、利用者に入力させるようにしてもよいし、利用者端末１２０に内蔵されたＳＩＭカード、ＮＦＣ、又はＦｅｌｉＣａのＩＤを取得してパスワードとして利用してもよい。

【００８１】

また、例えば、データ処理部２０２で、上記のようにして取得したパスワードにより暗号鍵を保護する処理をするようにしてもよい。また、データ処理部２０２で、所在情報及び制限情報に関連付けるファイル名を、ファイルを一意に特定できる管理番号に置き換える処理をするようにしてもよい。また、紙媒体３０１に制限情報と共に上記管理番号を出力するようにしてもよい。また、例えば、データ処理部２０２で、ファイルの暗号化に用いた暗号鍵により所在情報（例えばＵＲＬ）を暗号化し、所在情報送信部２１０は、当該暗号化された所在情報を送信するようにしてもよい。この場合、利用者端末１２０では、制限情報取得部４０１で取得した暗号鍵により所在情報取得部４０２で取得した当該暗号化された所在情報を復号し、復号された所在情報に基づいて、暗号化されたファイルを取得するようにすればよい。

【００８２】

また、上記実施形態における暗号鍵の文字列化、暗号鍵の符号化、及び暗号鍵の分割は、必須ではなく、例えば、これらのいずれかのみを実施する構成としてもよいし、これらのいずれかを組み合わせて実施する構成としてもよいし、いずれも実施しない構成としてもよい。例えば、暗号鍵を直接符号化する構成としてもよいし、暗号鍵をＱＲコード化する場合は、暗号鍵を一旦文字列化した上で符号化する構成としてもよい。また、利用者端末１２０での制限情報の取得に際しては、利用者が制限情報を直接入力するようにしてもよい。

【００８３】

また、ダミー鍵を混在させて、例えば、９つの符号化された暗号鍵３０２（ＱＲコード）を生成する場合には、ファイルを暗号化するための１つの暗号鍵とファイルの暗号化には用いられない８つの暗号鍵とからこれらの９つの符号化された暗号鍵３０２を生成するようにしてもよい。

【００８４】

また、例えば、データ処理部２０２は３つの暗号鍵によりファイルを暗号化し、利用者端末１２０はこれらの３つの暗号鍵を取得してファイルを復号するとしてもよい。更にこの場合、ファイルの復号には、これら３つの暗号鍵を順不同に取得すればよいとしてもよいし、所定の順序で取得しなければ復号できないとしてもよい。

【００８５】

また、複数の符号化された暗号鍵３０２を印刷する場合の配置の指定は、例えば、利用者端末１２０を介して行われる構成としてもよい。この場合、利用者が、利用者端末１２０に備えられたタッチパネル、入力キー等から成る入力部を操作して利用者端末１２０に当該配置を指定する情報（番号）を入力すると、利用者端末１２０は、当該配置を指定する情報をネットワークを介して情報処理装置１１０に送信するようにすればよい。そして、情報処理装置１１０は、当該配置を指定する情報を取得し、これに基づいて、複数の符号化された暗号鍵３０２を配置し紙媒体３０１に出力するようにすればよい。またこの場合、例えば、符号化された暗号鍵３０２の印刷の際に、当該配置を指定する情報を情報処

理装置１１０に入力することを利用者に求め、入力された情報が当該配置を指定する情報に一致したときに、符号化された暗号鍵３０２の印刷が実行されるようにしてもよい。更に、例えば、当該配置を指定する情報を利用者端末１２０で記憶しておき、利用者端末１２０で暗号鍵を取得した際の撮像順が当該情報で指定された順序に一致した場合に制限情報の取得を受け付けるようにしてもよい。

【００８６】

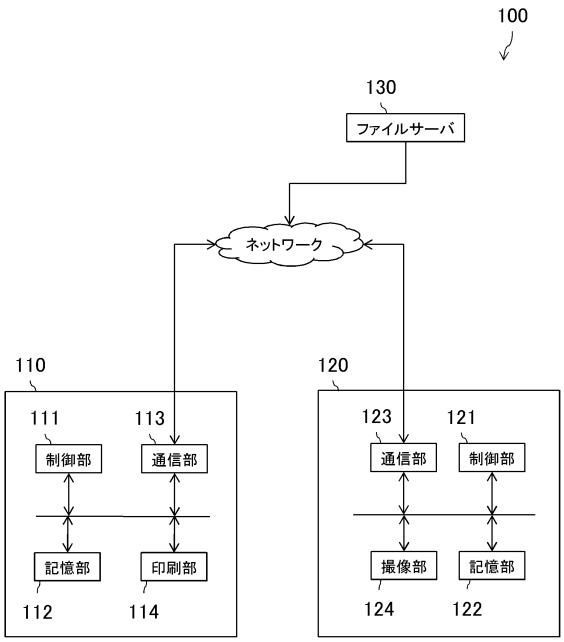
また、利用者端末１２０では、復号されたファイルは保存されないようにし、利用者端末１２０側でファイルを更新した場合は、利用者端末１２０側で情報処理装置１１０と同様の処理を行ってファイルを暗号化し、ファイルサーバ１３０に保存するようにしてもよい。こうすることで、利用者端末１２０に復号されたファイルが残らないため、データの漏洩が更に防止される

【符号の説明】

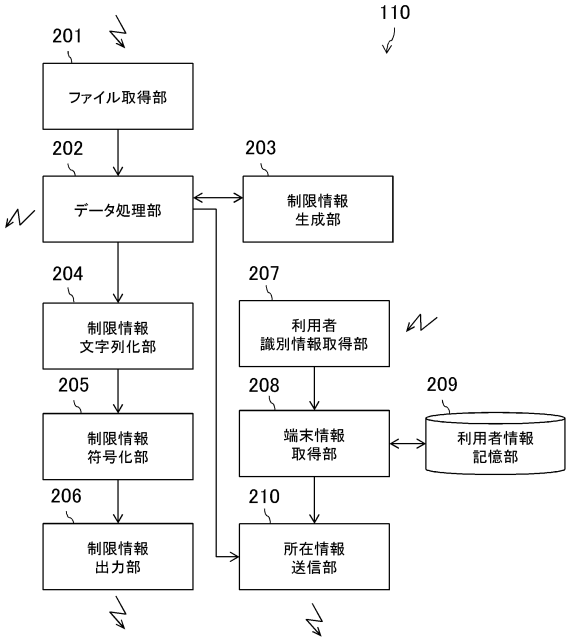
【００８７】

１００　情報処理システム、１１０　情報処理装置、１１１　制御部、１１２　記憶部、１１３　通信部、１１４　印刷部、１２０　利用者端末、１２１　制御部、１２２　記憶部、１２３　通信部、１２４　撮像部、１３０　ファイルサーバ、２０１　ファイル取得部、２０２　データ処理部、２０３　制限情報生成部、２０４　制限情報文字列化部、２０５　制限情報符号化部、２０６　制限情報出力部、２０７　利用者識別情報取得部、２０８　端末情報取得部、２０９　利用者情報記憶部、２１０　所在情報送信部、２１１　制限情報分割部、３０１　紙媒体、３０２　符号化された暗号鍵、４０１　制限情報取得部、４０２　所在情報取得部、４０３　端末側ファイル取得部、４０４　制限解除部。

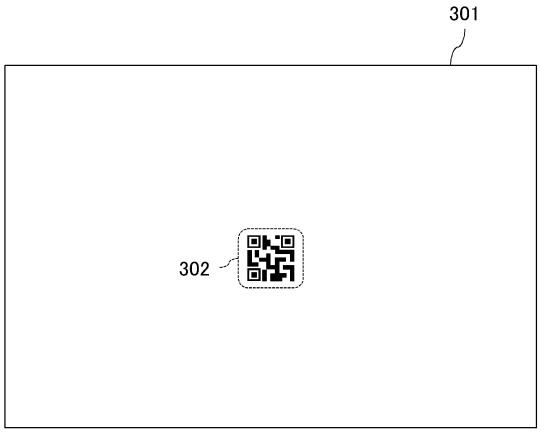
【図１】



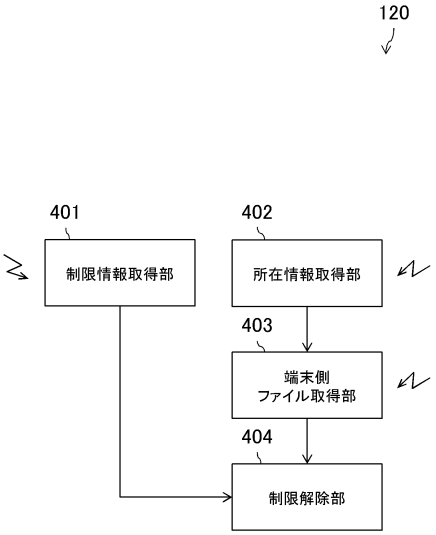
【図２】



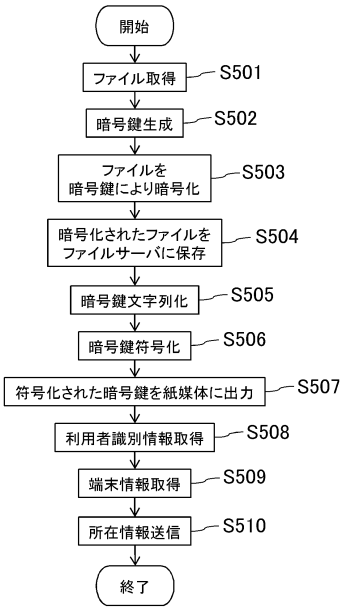
【図３】


301
302

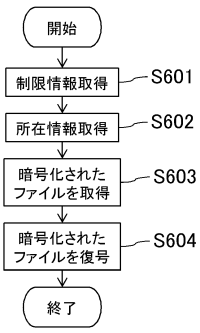
【図４】


120
401
制限情報取得部
402
所在情報取得部
403
端末側
ファイル取得部
404
制限解除部

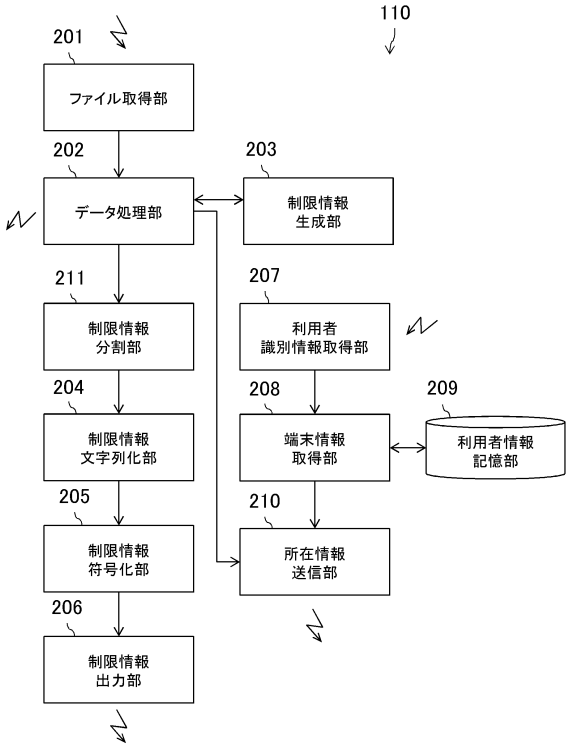
【図５】


開始
ファイル取得
S501
暗号鍵生成
S502
ファイルを
暗号鍵により暗号化
S503
暗号化されたファイルを
ファイルサーバに保存
S504
暗号鍵文字列化
S505
暗号鍵符号化
S506
符号化された暗号鍵を紙媒体に出力
S507
利用者識別情報取得
S508
端末情報取得
S509
所在情報送信
S510
終了

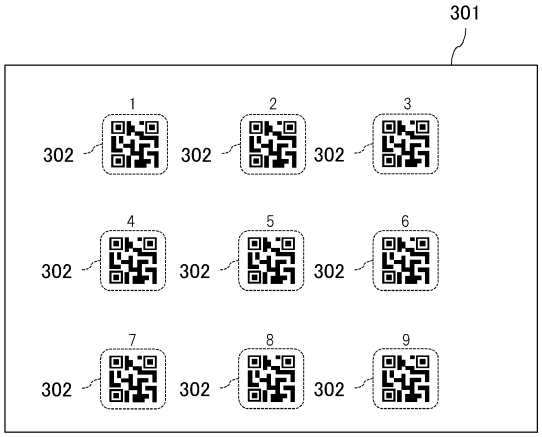
【図６】


開始
制限情報取得
S601
所在情報取得
S602
暗号化された
ファイルを取得
S603
暗号化された
ファイルを復号
S604
終了

【図７】


110
201
ファイル取得部
202
データ処理部
203
制限情報
生成部
211
制限情報
分割部
207
利用者
識別情報取得部
204
制限情報
文字列化部
208
端末情報
取得部
209
利用者情報
記憶部
205
制限情報
符号化部
210
所在情報
送信部
206
制限情報
出力部

【図８】


301
302
1
2
3
4
5
6
7
8
9

フロントページの続き

(56)参考文献 特開２００６－１７３７５３（ＪＰ，Ａ）
特開２０１２－２３１４５０（ＪＰ，Ａ）
特開２０１０－０４５６３７（ＪＰ，Ａ）
特開２０１０－１６０６１８（ＪＰ，Ａ）
特開２０１１－０１３９２１（ＪＰ，Ａ）
特開２００２－２３６６１８（ＪＰ，Ａ）
特開２００８－２２９９７７（ＪＰ，Ａ）
特表２００３－５１４４９０（ＪＰ，Ａ）
米国特許出願公開第２０１２／０２７８６１６（ＵＳ，Ａ１）
米国特許出願公開第２０１０／０１７４６８９（ＵＳ，Ａ１）
米国特許第０６８３１９８２（ＵＳ，Ｂ１）
特開２０１１－１９３３１９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６０
Ｇ０６Ｆ　１２／００