(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2010-3044
(P2010-3044A)
(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 21/24	(2006.01)	G06F	12/14	530D	5B017
		G06F	12/14	540A	

審査請求 未請求　請求項の数 8　ＯＬ　（全 16 頁）

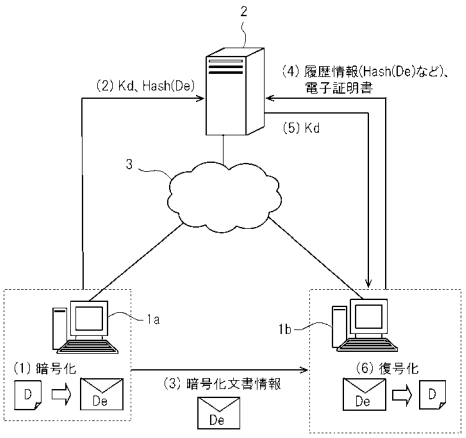
(21)出願番号　特願2008-160135 (P2008-160135)
(22)出願日　平成20年6月19日 (2008.6.19)

(71)出願人　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　増田　佳弘
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

Ｆターム(参考)　5B017 AA03　BA05　BA07　CA16

(54)【発明の名称】文書追跡システム、利用者端末、文書管理サーバおよびプログラム

(57)【要約】
【課題】企業間で交換した文書情報の操作を把握することができ、かつ運用に必要な手間の軽減を図ることが可能になる文書追跡システム等を提供すること。
【解決手段】利用者端末１と文書管理サーバ２からなる文書追跡システムを提供した。利用者端末１は、文書情報が暗号化されてなる暗号化文書情報の特徴値を生成する手段と、利用者端末１の操作者を特定しかつ前記操作者の正当性を示す操作者情報を取得する手段と、その特徴値および操作者情報を含む閲覧管理情報を文書管理サーバ２に送信する手段と、文書管理サーバ２から復号化用鍵情報を受信し復号化する手段と、を含み、文書管理サーバ２は、閲覧管理情報を受信する手段と、操作者を認証する手段と、特徴値に関連づけられた復号化用鍵情報を取得し、利用者端末１に送信する手段と、少なくとも操作者の情報を記憶する手段と、を含むことを特徴とする。
【選択図】図１



【特許請求の範囲】
【請求項１】
利用者端末と文書管理サーバからなる文書追跡システムであって、
前記利用者端末は、
閲覧対象となる文書情報が暗号化されてなる暗号化閲覧文書情報を取得する手段と、
前記暗号化閲覧文書情報の特徴値を生成する手段と、
前記利用者端末の操作者を特定しかつ前記操作者の正当性を示す操作者情報を取得する手段と、
前記暗号化閲覧文書情報の特徴値および前記操作者情報を含む閲覧管理情報を前記文書管理サーバに送信する閲覧管理情報送信手段と、
前記文書管理サーバから送信される復号化用鍵情報を受信する鍵受信手段と、
前記復号化用鍵情報に基づいて前記暗号化閲覧文書情報を復号化する手段と、
を含み、
前記文書管理サーバは、
前記閲覧管理情報送信手段より前記閲覧管理情報を受信する閲覧管理情報受信手段と、
前記閲覧管理情報に含まれる前記操作者情報に基づいて、前記操作者を認証する認証手段と、
前記操作者が認証される場合に、鍵情報記憶手段より前記暗号化閲覧文書情報の特徴値に関連づけられた復号化用鍵情報を取得し、前記利用者端末に前記復号化用鍵情報を送信する鍵応答送信手段と、
前記閲覧管理情報を受信する場合には、管理情報として少なくとも前記閲覧管理情報に含まれる前記操作者情報に応じた前記操作者の情報を取得する管理情報取得手段と、
前記管理情報を記憶する管理情報記憶手段と、
を含むことを特徴とする文書追跡システム。
【請求項２】
前記利用者端末は、
新規に作成された文書情報である新規文書情報を取得する手段と、
前記新規文書情報に対応する暗号化用鍵情報および復号化用鍵情報を生成する手段と、
前記新規文書情報に対応する暗号化用鍵情報に基づいて前記新規文書情報を暗号化してなる情報を暗号化新規文書情報として生成する手段と、
前記暗号化新規文書情報の特徴値を生成する手段と、
前記暗号化新規文書情報の特徴値と前記暗号化新規文書情報に対する復号化用鍵情報を通信によりアクセス可能な前記鍵情報記憶手段に格納する手段と、
をさらに含むことを特徴とする請求項１に記載の文書追跡システム。
【請求項３】
前記文書管理サーバは、
前記管理情報取得手段は、前記暗号化新規文書情報に対する復号化用鍵情報が前記鍵情報記憶手段に格納される場合には、少なくとも管理情報として前記新規文書情報を示す情報を取得する、
ことを特徴とする請求項２に記載の文書追跡システム。
【請求項４】
前記利用者端末は、
復号化された文書情報である編集対象文書情報が編集され編集済文書情報が生成されたことを検出する手段と、
前記生成された編集済文書情報に対応する暗号化用鍵情報および復号化用鍵情報を生成する手段と、
前記編集済文書情報に対する暗号化用鍵情報に基づいて前記編集済文書情報を暗号化してなる情報を暗号化編集済文書情報として生成する手段と、
前記暗号化編集済文書情報の特徴値を生成する手段と、
前記暗号化編集済文書情報の特徴値と前記暗号化編集済文書情報に対する復号化用鍵情

報を通信によりアクセス可能な鍵情報記憶手段に格納する手段と、
前記編集済文書情報を示す情報および前記編集対象文書情報を示す情報を含む編集管理情報を前記文書管理サーバに送信する編集管理情報送信手段と、
をさらに含み、
前記文書管理サーバは、
前記編集管理情報送信手段より前記編集管理情報を受信する編集管理情報受信手段、
をさらに含み、
前記管理情報取得手段は、前記編集管理情報を受信する場合には、管理情報として少なくとも前記編集済文書情報を示す情報および前記編集対象文書情報を示す情報を取得し、前記閲覧管理情報を受信する場合には、管理情報として少なくとも前記閲覧文書情報を示す情報および前記閲覧管理情報に含まれる前記操作者情報に応じた前記操作者の情報を取得する、
ことを特徴とする請求項１から３のいずれか一項に記載の文書追跡システム。
【請求項５】
閲覧対象となる文書情報が暗号化されてなる暗号化閲覧文書情報を取得する手段と、
前記暗号化閲覧文書情報の特徴値を生成する手段と、
前記利用者端末の操作者を特定しかつ前記操作者の正当性を示す操作者情報を取得する手段と、
前記暗号化閲覧文書情報の特徴値および前記操作者情報を含む閲覧管理情報を前記文書管理サーバに送信する閲覧管理情報送信手段と、
前記文書管理サーバから送信される復号化用鍵情報を受信する鍵受信手段と、
前記復号化用鍵情報に基づいて前記暗号化閲覧文書情報を復号化する手段と、
を含むことを特徴とする利用者端末。
【請求項６】
利用者端末より閲覧管理情報を受信する閲覧管理情報受信手段と、
前記閲覧管理情報に含まれる操作者情報に基づいて、操作者を認証する認証手段と、
前記操作者が認証される場合に、鍵情報記憶手段より前記文書情報の特徴値に関連づけられた復号化用鍵情報を取得し、前記利用者端末に前記復号化用鍵情報を送信する鍵応答送信手段と、
前記閲覧管理情報を受信する場合には、管理情報として少なくとも前記閲覧管理情報に含まれる前記操作者情報に応じた前記操作者の情報を取得する管理情報取得手段と、
前記管理情報を記憶する管理情報記憶手段と、
を含むことを特徴とする文書管理サーバ。
【請求項７】
閲覧対象となる文書情報が暗号化されてなる暗号化閲覧文書情報を取得する手段、
前記暗号化閲覧文書情報の特徴値を生成する手段、
前記利用者端末の操作者を特定しかつ前記操作者の正当性を示す操作者情報を取得する手段、
前記暗号化閲覧文書情報の特徴値および前記操作者情報を含む閲覧管理情報を前記文書管理サーバに送信する閲覧管理情報送信手段、
前記文書管理サーバから送信される復号化用鍵情報を受信する鍵受信手段、及び、
前記復号化用鍵情報に基づいて前記暗号化閲覧文書情報を復号化する手段、
としてコンピュータを機能させるためのプログラム。
【請求項８】
利用者端末より閲覧管理情報を受信する閲覧管理情報受信手段、
前記閲覧管理情報に含まれる操作者情報に基づいて、操作者を認証する認証手段、
前記操作者が認証される場合に、鍵情報記憶手段より前記文書情報の特徴値に関連づけられた復号化用鍵情報を取得し、前記利用者端末に前記復号化用鍵情報を送信する鍵応答送信手段、
前記閲覧管理情報を受信する場合には、管理情報として少なくとも前記閲覧管理情報に

含まれる前記操作者情報に応じた前記操作者の情報を取得する管理情報取得手段、及び、
前記管理情報を記憶する管理情報記憶手段、
としてコンピュータを機能させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は文書追跡システム、利用者端末、文書管理サーバおよびプログラムに関する。
【背景技術】
【０００２】
デジタル化された文書情報を管理するために、例えば所定の者以外に閲覧させないためのアクセス権限の管理や、デジタル文書に対し行われた編集の版の管理などが行われている。これらの管理を行うためのシステムとして、文書管理システムがある。従来の文書管理システムは企業内において運用することを前提としており、上述のアクセス権限や編集の版などは、企業内に設置した文書管理サーバで集中的に管理されていた。
【特許文献１】特開平８－２９２９６１号公報
【発明の開示】
【発明が解決しようとする課題】
【０００３】
近年、個人情報保護法などの法整備や社会のセキュリティに対する意識の変化などにより、企業間で交換した文書情報が相手先企業でどのように扱われているかを把握することが求められている。この対応方法として文書管理システムを適用することが考えられるが、文書管理システムは企業内での運用のように、例えば利用者端末やそれを操作する操作者の流動性が小さい状況を前提としている。このため利用者端末も操作者も流動的である企業間で文書管理システムを運用する場合、例えば操作者情報の管理負担や文書ＩＤ管理負担などの運用上の問題に直面することになる。
【０００４】
本発明は上記課題に鑑みてなされたものであって、その目的は、企業間で交換した文書情報の操作を把握することができ、かつ運用に必要な手間の軽減を図ることが可能になる文書追跡システム、利用者端末、文書管理サーバおよびプログラムを提供することにある。
【課題を解決するための手段】
【０００５】
請求項１の発明は利用者端末と文書管理サーバからなる文書追跡システムであって、前記利用者端末は、閲覧対象となる文書情報が暗号化されてなる暗号化閲覧文書情報を取得する手段と、前記暗号化閲覧文書情報の特徴値を生成する手段と、前記利用者端末の操作者を特定しかつ前記操作者の正当性を示す操作者情報を取得する手段と、前記暗号化閲覧文書情報の特徴値および前記操作者情報を含む閲覧管理情報を前記文書管理サーバに送信する閲覧管理情報送信手段と、前記文書管理サーバから送信される復号化用鍵情報を受信する鍵受信手段と、前記復号化用鍵情報に基づいて前記暗号化閲覧文書情報を復号化する手段と、を含み、前記文書管理サーバは、前記閲覧管理情報送信手段より前記閲覧管理情報を受信する閲覧管理情報受信手段と、前記閲覧管理情報に含まれる前記操作者情報に基づいて、前記操作者を認証する認証手段と、前記操作者が認証される場合に、鍵情報記憶手段より前記暗号化閲覧文書情報の特徴値に関連づけられた復号化用鍵情報を取得し、前記利用者端末に前記復号化用鍵情報を送信する鍵応答送信手段と、前記閲覧管理情報を受信する場合には、管理情報として少なくとも前記閲覧管理情報に含まれる前記操作者情報に応じた前記操作者の情報を取得する管理情報取得手段と、前記管理情報を記憶する管理情報記憶手段と、を含むことを特徴とする。
【０００６】
請求項２の発明は請求項１に記載の文書追跡システムであって、前記利用者端末は、新規に作成された文書情報である新規文書情報を取得する手段と、前記新規文書情報に対応

する暗号化用鍵情報および復号化用鍵情報を生成する手段と、前記新規文書情報に対応する暗号化用鍵情報に基づいて前記新規文書情報を暗号化してなる情報を暗号化新規文書情報として生成する手段と、前記暗号化新規文書情報の特徴値を生成する手段と、前記暗号化新規文書情報の特徴値と前記暗号化新規文書情報に対する復号化用鍵情報を通信によりアクセス可能な前記鍵情報記憶手段に格納する手段と、をさらに含むことを特徴とする。

【０００７】

請求項３の発明は請求項２に記載の文書追跡システムであって、前記文書管理サーバは、前記管理情報取得手段は、前記暗号化新規文書情報に対する復号化用鍵情報が前記鍵情報記憶手段に格納される場合には、少なくとも管理情報として前記新規文書情報を示す情報を取得する、ことを特徴とする。

【０００８】

請求項４の発明は請求項１から３のいずれか一項に記載の文書追跡システムであって、前記利用者端末は、復号化された文書情報である編集対象文書情報が編集され編集済文書情報が生成されたことを検出する手段と、前記生成された編集済文書情報に対応する暗号化用鍵情報および復号化用鍵情報を生成する手段と、前記編集済文書情報に対する暗号化用鍵情報に基づいて前記編集済文書情報を暗号化してなる情報を暗号化編集済文書情報として生成する手段と、前記暗号化編集済文書情報の特徴値を生成する手段と、前記暗号化編集済文書情報の特徴値と前記暗号化編集済文書情報に対する復号化用鍵情報を通信によりアクセス可能な鍵情報記憶手段に格納する手段と、前記編集済文書情報を示す情報および前記編集対象文書情報を示す情報を含む編集管理情報を前記文書管理サーバに送信する編集管理情報送信手段と、をさらに含み、前記文書管理サーバは、前記編集管理情報送信手段より前記編集管理情報を受信する編集管理情報受信手段、をさらに含み、前記管理情報取得手段は、前記編集管理情報を受信する場合には、管理情報として少なくとも前記編集済文書情報を示す情報および前記編集対象文書情報を示す情報を取得し、前記閲覧管理情報を受信する場合には、管理情報として少なくとも前記閲覧文書情報を示す情報および前記閲覧管理情報に含まれる前記操作者情報に応じた前記操作者の情報を取得する、ことを特徴とする。

【０００９】

請求項５の発明は利用者端末であって、閲覧対象となる文書情報が暗号化されてなる暗号化閲覧文書情報を取得する手段と、前記暗号化閲覧文書情報の特徴値を生成する手段と、前記利用者端末の操作者を特定しかつ前記操作者の正当性を示す操作者情報を取得する手段と、前記暗号化閲覧文書情報の特徴値および前記操作者情報を含む閲覧管理情報を前記文書管理サーバに送信する閲覧管理情報送信手段と、前記文書管理サーバから送信される復号化用鍵情報を受信する鍵受信手段と、前記復号化用鍵情報に基づいて前記暗号化閲覧文書情報を復号化する手段と、を含むことを特徴とする。

【００１０】

請求項６の発明は文書管理サーバであって、利用者端末より閲覧管理情報を受信する閲覧管理情報受信手段と、前記閲覧管理情報に含まれる操作者情報に基づいて、操作者を認証する認証手段と、前記操作者が認証される場合に、鍵情報記憶手段より前記文書情報の特徴値に関連づけられた復号化用鍵情報を取得し、前記利用者端末に前記復号化用鍵情報を送信する鍵応答送信手段と、前記閲覧管理情報を受信する場合には、管理情報として少なくとも前記閲覧管理情報に含まれる前記操作者情報に応じた前記操作者の情報を取得する管理情報取得手段と、前記管理情報を記憶する管理情報記憶手段と、を含むことを特徴とする。

【００１１】

請求項７の発明は閲覧対象となる文書情報が暗号化されてなる暗号化閲覧文書情報を取得する手段、前記暗号化閲覧文書情報の特徴値を生成する手段、前記利用者端末の操作者を特定しかつ前記操作者の正当性を示す操作者情報を取得する手段、前記暗号化閲覧文書情報の特徴値および前記操作者情報を含む閲覧管理情報を前記文書管理サーバに送信する閲覧管理情報送信手段、前記文書管理サーバから送信される復号化用鍵情報を受信する鍵

受信手段、及び、前記復号化用鍵情報に基づいて前記暗号化閲覧文書情報を復号化する手段、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る。

【００１２】

請求項８の発明は利用者端末より閲覧管理情報を受信する閲覧管理情報受信手段、前記閲覧管理情報に含まれる操作者情報に基づいて、操作者を認証する認証手段、前記操作者が認証される場合に、鍵情報記憶手段より前記文書情報の特徴値に関連づけられた復号化用鍵情報を取得し、前記利用者端末に前記復号化用鍵情報を送信する鍵応答送信手段、前記閲覧管理情報を受信する場合には、管理情報として少なくとも前記閲覧管理情報に含まれる前記操作者情報に応じた前記操作者の情報を取得する管理情報取得手段、及び、前記管理情報を記憶する管理情報記憶手段、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る。

【発明の効果】

【００１３】

請求項１の発明によれば、利用者端末から送信された暗号化閲覧文書情報の特徴値と操作者情報によって、少なくとも文書情報を閲覧する操作者の情報を文書管理サーバで記憶することができる。

【００１４】

請求項２の発明によれば、新規に作成された文書情報を暗号化してなる情報の特徴値と、それに対応する復号化用鍵情報を利用者端末から登録することができる。

【００１５】

請求項３の発明によれば、利用者端末において文書が新規に作成されたことを文書管理サーバで記憶することができる。

【００１６】

請求項４の発明によれば、利用者端末において編集対象文書情報が編集され、編集済文書情報が生成されたことを文書管理サーバ側で記憶し、編集済文書情報を暗号化してなる情報の特徴値と、それに対応する復号化用鍵情報を利用者端末から登録することができる。

【００１７】

請求項５，７の発明によれば、利用者端末から文書管理サーバに文書情報を閲覧した操作者の情報を暗号化閲覧文書情報の特徴値とともに送ることができる。

【００１８】

請求項６，８の発明によれば、利用者端末から送信された操作者の情報を認証し、暗号化閲覧文書情報の特徴値に関連づけられた復号化用鍵情報を利用者端末に送信することができる。

【発明を実施するための最良の形態】

【００１９】

以下、本発明の実施形態について図面に基づき詳細に説明する。図１は、本実施形態に係る文書追跡システムの構成および処理の概略の一例を示す図である。同図に示すように、文書追跡システムは利用者端末１ａ，１ｂ（以下区別が必要な時を除き利用者端末１という）、文書管理サーバ２、ネットワーク３を含んでいる。利用者端末１は例えばパーソナルコンピュータ等によって、文書管理サーバ２は例えばサーバコンピュータ等によって実現される。ネットワーク３は例えばインターネット、ＬＡＮ（構内通信網）等で構成されており、利用者端末１と文書管理サーバ２との間の通信接続を提供している。

【００２０】

本実施形態においては、利用者端末１と文書管理サーバ２間で行われる処理の種類は、例えば企業間文書交換の対象となる文書情報を新規作成した際の処理（以下新規作成時処理という。同図（１）と（２）に相当）、暗号化された文書を閲覧する際の処理（以下閲覧時処理という。同図（４）から（６）に相当）、文書情報を編集した際の処理（以下編集時処理という。図示しない）の３種類に分けられる。

【００２１】

新規作成時処理を行う前に、利用者端末の操作者（以下新規操作者という）は事前に他企業への文書交換の対象となる文書情報Ｄを利用者端末１ａ内に準備する。新規作成時処理では、はじめに利用者端末１ａはその文書情報Ｄに対して暗号化用の鍵Ｋｅおよび復号化用の鍵Ｋｄを生成する。次に暗号化用の鍵Ｋｅを用いて文書情報Ｄを暗号化し暗号化文書情報Ｄｅを生成する（図１の（１））。次に利用者端末１ａは復号化用の鍵Ｋｄおよび暗号化文書情報の特徴値の一種であるハッシュ値Ｈａｓｈ（Ｄｅ）を文書管理サーバ２に送信する（同図の（２））。文書管理サーバ２は、受信したハッシュ値Ｈａｓｈ（Ｄｅ）をキーとして復号用の鍵Ｋｄを文書管理サーバ内に登録する。新規操作者は、新規作成時処理で得られた暗号化された文書情報Ｄｅを他企業にある利用者端末１ｂの操作者（以下閲覧操作者）にメール送信などの手段で送付する（同図の（３））。

【００２２】

閲覧操作者は暗号化文書情報Ｄｅを閲覧するために利用者端末１ｂに以下の閲覧時処理を行わせる。はじめに、利用者端末１ｂは送付された暗号化文書情報Ｄｅのハッシュ値Ｈａｓｈ（Ｄｅ）を含む履歴情報および閲覧操作者の正当性を証明する電子証明書を文書管理サーバ２に送信し（同図の（４））、文書管理サーバはそれらの情報を記録する。電子証明書によって閲覧操作者の正当性が認証されれば、文書管理サーバは上記ハッシュ値Ｈａｓｈ（Ｄｅ）をキーとして復号化用の鍵Ｋｄをデータベースから取得し、利用者端末１ｂに返信する（同図の（５））。利用者端末１ｂは受け取った復号用の鍵Ｋｄによって暗号化された文書情報Ｄｅを復号化してもとの文書情報Ｄを得る（同図の（６））。これにより、閲覧操作者は復号化された文書を閲覧、もしくは編集する。

【００２３】

上記新規作成時処理等を行った後に文書情報Ｄが編集（例えば変更など）される場合は、編集時処理を行う。編集時処理では、変更された文書の暗号化や復号化用の鍵の登録など新規作成時処理に行う処理と同様の処理（同図（１）と（２）参照）を行うほかに、変更前の文書情報と変更後の文書情報との関係を示す履歴情報を文書管理サーバ２に対して送信する処理等を行う。

【００２４】

以下、本実施形態にかかる文書追跡システムの詳細について説明する。図２は、本実施形態に係る利用者端末１の構成の一例を示す図である。利用者端末１は、ＣＰＵ１１、記憶部１２、通信部１３、入出力部１４を含んでいる。

【００２５】

ＣＰＵ１１は、記憶部１２に格納されているプログラムに従って動作する。なお、上記プログラムは、ＣＤ－ＲＯＭやＤＶＤ－ＲＯＭ等の情報記録媒体に格納されて提供されるものであってもよいし、インターネット等のネットワークを介して提供されるものであってもよい。

【００２６】

記憶部１２は、ＲＡＭやＲＯＭ等のメモリ素子およびハードディスクドライブ等によって構成されている。記憶部１２は、上記プログラムを格納する。また、記憶部１２は、各部から入力される情報や演算結果を格納する。

【００２７】

通信部１３は、他の装置と通信接続するための通信手段等で構成されている。通信部１３は、ＣＰＵ１１の制御に基づいて、他の装置から受信した情報をＣＰＵ１１や記憶部１２に入力し、他の装置に情報を送信（出力）する。

【００２８】

入出力部１４は、モニタやキーボード、マウス等の表示出力手段および入力手段等で構成されている。入出力部１４は、ＣＰＵ１１の制御に基づいて、画像データ等をモニタ等に表示（出力）し、キーボードやマウスより操作者からの情報を取得する。

【００２９】

図３は、本実施形態に係る文書管理サーバ２の構成の一例を示す図である。文書管理サーバ２は、ＣＰＵ２１、記憶部２２、通信部２３、入出力部２４を含んでいる。文書管理

サーバ２において、ＣＰＵ２１、記憶部２２、通信部２３、入出力部２４はそれぞれＣＰＵ１１、記憶部１２、通信部１３、入出力部１４と同様の構成であるため詳細な説明は省略する。

【００３０】

図４は、本実施形態に係る利用者端末１の機能ブロックを示す図である。利用者端末１は機能的に、新規作成時処理に関連する新規文書情報取得部４１、新管理情報生成送信部４２および新規鍵登録部４３と、閲覧時処理に関連する暗号化閲覧文書情報取得部４４、閲覧管理情報生成送信部４５、鍵受信部４６および復号化部４７と、編集時処理に関連する編集検出部４８、編集管理情報生成送信部４９および編集鍵登録部５０と、共通して用いられる鍵生成部５１および暗号化部５２と、を含む。これらの機能はＣＰＵ１１が記憶部１２に格納されたプログラムを実行し、通信部１３および入出力部１４を制御することによって実現される。なお、各機能の詳細は共通して用いられる機能を除き、文書管理サーバ２の機能とともに処理の種類毎に説明する。

【００３１】

鍵生成部５１は、ＣＰＵ１１、記憶部１２を中心として実現される。鍵生成部５１は他の機能から呼び出され、暗号化用の鍵情報と復号化用の鍵情報を生成する。例えば公開鍵暗号方式を用いる場合は、生成される鍵は秘密鍵が暗号化用の鍵情報であり公開鍵が復号化用の鍵情報となる。また、共通鍵暗号方式を用い、暗号化用の鍵情報と復号化用の鍵情報とが同じとなっても良い。

【００３２】

暗号化部５２は、ＣＰＵ１１、記憶部１２を中心として実現される。暗号化部５２は他の機能から呼び出され、上記生成された暗号化用の鍵情報を用いて指定された文書情報を暗号化し、暗号化文書情報を生成する。

【００３３】

図５は、本実施形態に係る文書管理サーバ２の機能ブロックを示す図である。文書管理サーバ２は機能的に、新規作成時処理に関連する新管理情報受信部６１と、閲覧時処理に関連する閲覧管理情報受信部６２および鍵応答送信部６３と、編集処理時に関連する編集管理情報受信部６４と、共通して用いられる管理情報取得部７１、認証部７２、管理情報記憶部７３および鍵情報記憶部７４と、を含む。これらの機能はＣＰＵ２１が記憶部２２に格納されたプログラムを実行し、通信部２３および入出力部２４を制御することによって実現される。

【００３４】

管理情報取得部７１は、ＣＰＵ２１、記憶部２２、通信部２３を中心として実現される。新規作成時処理、閲覧時処理および編集時処理のそれぞれにおいて利用者端末１から送信された情報（以下、それぞれ新管理情報、閲覧管理情報および編集管理情報という）から必要な情報を取得する。新管理情報、閲覧管理情報および編集管理情報は、それぞれ履歴情報と電子証明書情報とからなる。

【００３５】

図６および図７は、履歴情報のデータ形式の一例を示す図である。履歴ＩＤは、各履歴情報を一意に識別する情報であり、例えば、この履歴ＩＤを除く履歴情報の内容の特徴を示す値であるハッシュ値を求めることで取得してよい。ハッシュ値の計算方法としては、例えばＳＨＡ－２５６など、ハッシュ値どうしが衝突する確率が十分に小さい方法を選択すればよい。本図の例では、履歴情報の内容はＸＭＬ形式で表されている。ｕｓｅｒタグの値は操作者情報の一種である操作者の名称を表している。ｔｉｍｅｓｔａｍｐタグの値は、この履歴情報が作成される日時を表す。この項目については、編集時処理の場合などは、代わりに文書情報が編集された日時としてもよい。ｍｅｔｈｏｄタグの値は、新規作成時処理、閲覧時処理又は編集時処理の種類を表している。ここで、種類は前述の３種類だけではなく、例えば変更、コピーなど編集時処理の詳細について細かく表すようにしてもよい。ｂｏｄｙタグの値は、暗号化文書情報の特徴値が格納されている。暗号化文書情報の特徴値は、文書情報を一意に識別できる値である必要があり、例えば上述のハッシュ

値を用いればよい。ｂａｓｅタグの値は、この文書情報に関連して直前に送られた履歴情報の履歴ＩＤである。これによって、直前に行われた操作と関連づけをしている。ｆｉｌｅｎａｍｅタグの値は、利用者端末上の文書情報のファイルのファイル名を格納している。ここで、ｂｏｄｙタグにより文書情報と履歴ＩＤが紐付けられている。つまり、編集時処理では履歴ＩＤは編集対象となった文書情報も示し、ｂａｓｅタグの値は編集済の文書情報も示すことになる。なお、履歴情報の項目には、暗号化されていない文書情報の特徴値や、文書ファイルのサイズなど、文書を追跡する際に有用と思われる項目を追加してもよい。各項目の取得方法の詳細については後述する。

【００３６】

電子証明書情報は操作者情報の一種であり、操作者を特定しかつ操作者の正当性を表すことができる。電子証明書は例えば第三者の認証機関（ＣＡ）によって各操作者に対し発行される。

【００３７】

認証部７２は、ＣＰＵ２１、記憶部２２、通信部２３を中心として実現される。認証部７２は、管理情報取得部７１で取得した情報を用いて、操作者の正当性を認証する。認証は、例えば、電子証明書を用いる公知の手法などによって行う。認証に必要な情報は電子証明書およびそれと同時に受信した情報に含まれているため、操作者を認証するための情報をデータベースとして準備しておく必要はない。

【００３８】

管理情報記憶部７３は、ＣＰＵ２１、記憶部２２を中心として実現される。管理情報取得部７１が新規作成時処理、閲覧時処理、編集時処理のそれぞれの場合に対して取得した管理情報を記憶する。

【００３９】

鍵情報記憶部７４は、ＣＰＵ２１、記憶部２２、通信部２３を中心として実現される。通信部２３を用いて新規作成時処理、編集時処理に利用者端末から送られる暗号化文書情報の特徴値と復号化用鍵情報とを取得し、暗号化文書情報の特徴値と関連づけて復号化用鍵情報を記憶部２２に記憶する。また、他の機能ブロックから指定された暗号化文書情報の特徴値に対応する復号化用鍵情報を記憶部２２から取得し、呼び出し元の機能ブロックに渡す。

【００４０】

以下では、処理の種類ごとに処理フローとともに関連する機能ブロックについて説明していく。ここで図８は新規作成処理時における利用者端末１の処理フローの一例を示す図である。

【００４１】

新規文書情報取得部４１は、ＣＰＵ１１、記憶部１２、入出力部１４を中心として実現される。新規文書情報取得部４１は操作者が文書交換の対象として準備した文書情報（以下「新規文書情報」という）として記憶部１２や入出力部１４から取得する（Ｓ１０１）。

【００４２】

新管理情報生成送信部４２は、ＣＰＵ１１、記憶部１２、通信部１３を中心として実現される。新管理情報生成送信部４２は、鍵生成部５１を呼び出して、取得した新規文書情報に対する暗号化用の鍵情報と復号化用の鍵情報を生成する（Ｓ１０２）。生成された暗号化用鍵情報を用いて暗号化部５２を呼び出して新規文書情報を暗号化し（Ｓ１０３）、さらに新規文書情報が暗号化された情報の特徴値としてハッシュ値を生成する（Ｓ１０４）。次に、記憶部１２に予め記憶されている操作者に対応した電子証明書情報を取得する（Ｓ１０５）。次に新管理情報を生成する（Ｓ１０６）。具体的には、例えば図７に示されるような履歴情報を電子証明書情報でデジタル署名し、電子証明書情報を添付することで新管理情報を生成する。履歴情報の各項目について、例えばｕｓｅｒタグには証明書情報から取得したユーザ名の情報が、ｔｉｍｅｓｔａｍｐタグには履歴情報の作成日時が、ｍｅｔｈｏｄタグには新規作成処理時であることを示す文字列が、ｂｏｄｙタグには新規

文書情報が暗号化された情報の特徴値が格納されている。そして、生成された新管理情報を文書管理サーバ２に送信する（Ｓ１０７）。

【００４３】

新規鍵登録部４３は、ＣＰＵ１１、記憶部１２、通信部１３を中心として実現される。鍵生成部５１で生成された復号化用鍵情報を、新規文書情報が暗号化された情報の特徴値とともに文書管理サーバ２の鍵情報記憶部７４に送信し、鍵情報記憶部７４にその情報を格納させる（Ｓ１０８）。

【００４４】

図９は、新規作成処理時における文書管理サーバ２の処理フローの一例を示す図である。新管理情報受信部６１は、ＣＰＵ２１、記憶部２２、通信部２３を中心として実現される。新管理情報受信部６１は、通信部２３を通じて利用者端末１の新管理情報生成送信部４２から新管理情報を受信する（Ｓ１１１）。

【００４５】

管理情報取得部７１は、新規作成処理時には、受信した新管理情報から、格納対象の情報である管理情報を抽出する（Ｓ１１２）。管理情報の項目としては、例えば、図７に示される履歴情報の履歴ＩＤ、ｂｏｄｙタグの値、ｔｉｍｅｓｔａｍｐタグの値、ｆｉｌｅｎａｍｅタグの値、ｕｓｅｒタグの値や、電子証明書から取得する操作者を特定する文字列がある。そして、管理情報記憶部７３は、それらの項目からなる管理情報を記憶する（Ｓ１１３）。なお、記憶する前に認証部７２によって操作者の認証を行い、正当でない場合にはその旨を記憶するようにしてもよい。

【００４６】

図１０は閲覧処理時における利用者端末１の処理フローの一例を示す図である。暗号化閲覧文書情報取得部４４は、ＣＰＵ１１、記憶部１２、入出力部１４を中心として実現される。暗号化閲覧文書情報取得部４４は先ほどの新規作成処理時などに作成された閲覧対象となる暗号化された文書情報（以下「暗号化閲覧文書情報」という）を記憶部１２や入出力部１４などから取得する（Ｓ１２１）。なお、暗号化閲覧文書情報は、新規作成処理時の操作をした操作者から、電子メール等の文書追跡システムが直接管理しない方法で予め取得する。

【００４７】

閲覧管理情報生成送信部４５は、ＣＰＵ１１、記憶部１２、通信部１３を中心として実現される。閲覧管理情報生成送信部４５は、はじめに暗号化閲覧文書情報の特徴値としてハッシュ値を生成し（Ｓ１２２）、記憶部１２に予め記憶されている、操作者に対応した電子証明書情報を取得する（Ｓ１２３）。次に閲覧管理情報を生成する（Ｓ１２４）。具体的には閲覧管理情報は、例えば図６の閲覧時の欄に示されるような履歴情報を電子証明書情報でデジタル署名し、電子証明書情報を添付して生成する。履歴情報の各項目について、例えばｕｓｅｒタグには証明書情報から抽出したユーザ名の情報が、ｔｉｍｅｓｔａｍｐタグには履歴情報の作成日時が、ｍｅｔｈｏｄタグには閲覧処理時であることを示す文字列が、ｂｏｄｙタグには暗号化閲覧文書情報の特徴値が格納されている。そして、生成された閲覧管理情報を文書管理サーバ２に送信する（Ｓ１２５）。

【００４８】

図１１は、閲覧処理時における文書管理サーバ２の処理フローの一例を示す図である。

閲覧管理情報受信部６２は、ＣＰＵ２１、記憶部２２、通信部２３を中心として実現される。閲覧管理情報受信部６２は、利用者端末１の閲覧管理情報生成送信部４５から閲覧管理情報を受信する（Ｓ１３１）。

【００４９】

管理情報取得部７１は、閲覧処理時には、その閲覧管理情報から、格納対象の情報である管理情報を抽出する（Ｓ１３２）。管理情報の項目としては、例えば、図６に示される履歴情報の履歴ＩＤ、ｂｏｄｙタグの値、ｔｉｍｅｓｔａｍｐタグの値、ｆｉｌｅｎａｍｅタグの値、ｕｓｅｒタグの値や、電子証明書から取得する操作者を特定する文字列がある。管理情報記憶部７３は、管理情報取得部７１で抽出された項目からなる管理情報を記

憶する（Ｓ１３３）。

【００５０】

鍵応答送信部６３は、ＣＰＵ２１、記憶部２２、通信部２３を中心として実現される。鍵応答送信部６３は、認証部７２を用いて操作者が正当であるか認証する（Ｓ１３４）。正当である場合にはｂｏｄｙタグの値としても含まれている暗号化閲覧文書情報の特徴値を用いて鍵情報記憶部７４より復号化用鍵情報を取得し（Ｓ１３５）、利用者端末１に復号化用鍵情報を送信する（Ｓ１３６）。

【００５１】

利用者端末１の鍵受信部４６は、ＣＰＵ１１、記憶部１２、通信部１３を中心として実現される。文書管理サーバ２の鍵応答送信部６３から送信された復号化用鍵情報を受信する（Ｓ１２６）。

【００５２】

復号化部４７は、ＣＰＵ１１、記憶部１２を中心として実現される。受信した復号化用鍵情報を用いて、暗号化閲覧文書情報を復号化する（Ｓ１２７）。

【００５３】

図１２は編集処理時における利用者端末１の処理フローの一例を示す図である。編集検出部４８は、ＣＰＵ１１、記憶部１２、入出力部１４を中心として実現される。編集検出部４８は操作者が行った文書情報（以下「編集対象文書情報」という）に対する編集操作を検出する（Ｓ１４１）。編集操作を検出するには、例えば予め編集対象文書情報のファイルのタイムスタンプを記憶しておき、何らかのタイミングでそのタイムスタンプが変更されているか確認するなどの公知の手法を用いて行う。次に、その編集対象文書情報の編集前のファイルに対応する履歴情報の履歴ＩＤを取得する（Ｓ１４２）。図１４はその履歴ＩＤを取得するために利用者端末１に記憶される情報の例である。本図のように編集対象文書情報のファイルパスとそのファイルに対してされた直前の操作に対応する履歴ＩＤを記憶しておくことで、編集操作がされたファイルに対応する文書情報（以下「編集済文書情報」という）の編集前の文書である編集対象文書情報に対応する履歴ＩＤを取得することができる。なお、これらの情報は、新規作成処理時、閲覧処理時、編集処理時のそれぞれ履歴情報を作成する際に生成、更新するようにすればよい。

【００５４】

編集管理情報生成送信部４９は、ＣＰＵ１１、記憶部１２、通信部１３を中心として実現される。編集管理情報生成送信部４９は、鍵生成部５１を呼び出して、編集済文書情報に対する暗号化用の鍵情報と復号化用の鍵情報を生成する（Ｓ１４３）。生成された暗号化用鍵情報を用いて暗号化部５２を呼び出して編集済文書情報を暗号化し（Ｓ１４４）、さらに編集済文書情報が暗号化された情報の特徴値としてハッシュ値を生成する（Ｓ１４５）。記憶部１２に予め記憶されている、操作者に対応した電子証明書情報を取得する（Ｓ１４６）。次に編集管理情報を生成する（Ｓ１４７）。具体的には、例えば図６の編集時欄に示されるような履歴情報を電子証明書情報でデジタル署名し、電子証明書情報を添付することで生成する。履歴情報の各項目について、例えばｕｓｅｒタグには証明書情報から取得したユーザ名の情報が、ｔｉｍｅｓｔａｍｐタグには履歴情報の作成日時が、ｍｅｔｈｏｄタグには新規作成処理時であることを示す文字列が、ｂａｓｅタグには編集対象文書情報に対応する履歴ＩＤが、ｂｏｄｙタグには編集済文書情報が暗号化された情報の特徴値が格納されている。そして、生成された編集管理情報を文書管理サーバ２に送信する（Ｓ１４８）。

【００５５】

編集鍵登録部５０は、ＣＰＵ１１、記憶部１２、通信部１３を中心として実現される。鍵生成部５１で生成された復号化用鍵情報を、編集済文書情報が暗号化された情報の特徴値とともに文書管理サーバ２の鍵情報記憶部７４に送信し、鍵情報記憶部７４にその情報を格納させる（Ｓ１４９）。

【００５６】

図１３は、新規作成処理時における文書管理サーバ２の処理フローの一例を示す図であ

る。編集管理情報受信部６４は、ＣＰＵ２１、記憶部２２、通信部２３を中心として実現される。編集管理情報受信部６４は、利用者端末１の編集管理情報生成送信部４９から編集管理情報を受信する（Ｓ１５１）。

【００５７】

管理情報取得部７１は、編集処理時には、受信した編集管理情報から、格納対象の情報である管理情報を抽出する（Ｓ１５２）。管理情報の項目としては、例えば、図６に示される履歴情報の履歴ＩＤ、ｂａｓｅタグの値、ｂｏｄｙタグの値、ｔｉｍｅｓｔａｍｐタグの値、ｆｉｌｅｎａｍｅタグの値や、電子証明書から取得する操作者を特定する文字列がある。そして、管理情報記憶部７３は、それらの項目からなる管理情報を記憶する（Ｓ１５３）。なお、記憶する前に認証部７２によって操作者の認証を行い、正当でない場合にはその旨を記憶するようにしてもよい。

【００５８】

編集処理時には、ｂａｓｅタグの値に履歴ＩＤを格納することで、直前の操作との対応をとることが可能になる。さらに直前の操作との対応をとることで、編集前の文書情報との対応も取ることができる。例えば図６の閲覧時の履歴情報の履歴ＩＤが、編集時の履歴情報のｂａｓｅタグの欄に格納されている。これによって、編集によって文書情報が変化しｂｏｄｙタグの値が変化しても、事後的に元のファイルを追跡することが可能である。図１５は、操作者Ａｌｉｃｅが文書を編集し、編集済文書情報を暗号化した情報をＢｏｂに送付し、Ｂｏｂが閲覧した場合の履歴情報の例である。この例では閲覧時処理でｂａｓｅタグに情報が格納されないために、履歴ＩＤからは元の文書を追跡することができないが、文書情報が等しいためｂｏｄｙタグの値は等しく、事後的に元のファイルを追跡することができる。なお文書情報の追跡を確実に行うために、他人に送信可能な状態のファイルとして操作者が直接アクセスできるのは暗号化された文書情報のみにするよう利用者端末で制御する方が好適である。

【００５９】

これまで実施形態について説明してきたが、本発明はこの実施形態に限られるものではない。例えば、本実施形態では文書管理サーバで復号化用鍵も記憶しているが、他のサーバに分離してもよい。鍵の記憶自体は独立して可能な動作であるからである。また、復号化用鍵の記憶を文書管理サーバで管理する場合は、復号化用鍵情報と各種管理情報を一つの情報としてまとめて送受信するようにしてもよい。

【００６０】

なお、本実施形態で記載している文書情報の内容は、単なるテキスト文書には限られず、図形、音声、動画等も含む。ワードプロセッサ等のアプリケーションにおいて上記のものを分け隔て無く扱える以上、図形、音声、動画等を別扱いする必要は存在しないからである。

【図面の簡単な説明】

【００６１】

【図１】本実施形態に係る文書追跡システムの構成および処理の概略の一例を示す図である。

【図２】本実施形態に係る利用者端末の構成の一例を示す図である。

【図３】本実施形態に係る文書管理サーバの構成の一例を示す図である。

【図４】本実施形態に係る利用者端末の機能ブロックを示す図である。

【図５】本実施形態に係る文書管理サーバの機能ブロックを示す図である。

【図６】履歴情報のデータ形式の一例を示す図である。

【図７】履歴情報のデータ形式の一例を示す図である。

【図８】新規作成処理時における利用者端末の処理フローの一例を示す図である。

【図９】新規作成処理時における文書管理サーバの処理フローの一例を示す図である。

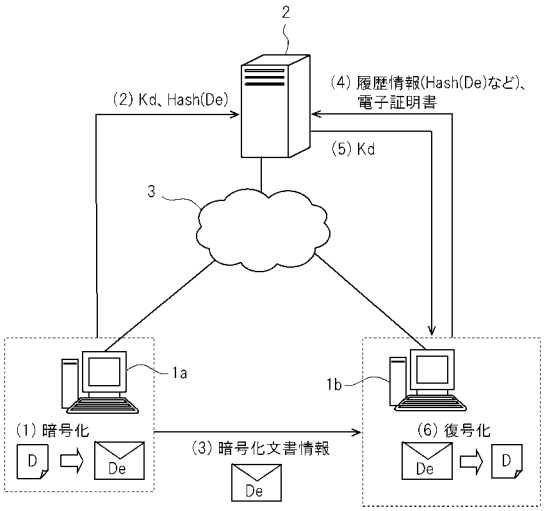
【図１０】閲覧処理時における利用者端末の処理フローの一例を示す図である。

【図１１】閲覧処理時における文書管理サーバの処理フローの一例を示す図である。

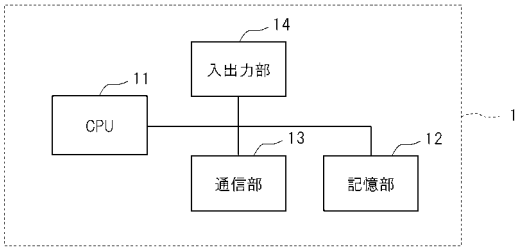
【図１２】編集処理時における利用者端末の処理フローの一例を示す図である。

【図１３】編集処理時における文書管理サーバの処理フローの一例を示す図である。
【図１４】履歴ＩＤを取得するために利用者端末に記憶される情報の例を示す図である。
【図１５】編集済文書情報を暗号化した情報を他者が閲覧した場合の履歴情報の例を示す図である。
【符号の説明】
【００６２】
１，１ａ，１ｂ　利用者端末、２　文書管理サーバ、３　ネットワーク、Ｄ　文書情報、Ｄｅ　暗号化文書情報、Ｋｄ　復号化用の鍵、１１，２１　ＣＰＵ、１２，２２　記憶部、１３，２３　通信部、１４，２４　入出力部、４１　新規文書情報取得部、４２　新管理情報生成送信部、４３　新規鍵登録部、４４　暗号化閲覧文書情報取得部、４５　閲覧管理情報生成送信部、４６　鍵受信部、４７　復号化部、４８　編集検出部、４９　編集管理情報生成送信部、５０　編集鍵登録部、５１　鍵生成部、５２　暗号化部、６１　新管理情報受信部、６２　閲覧管理情報受信部、６３　鍵応答送信部、６４　編集管理情報受信部、７１　管理情報受信部、７２　認証部、７３　管理情報記憶部、７４　鍵情報記憶部。

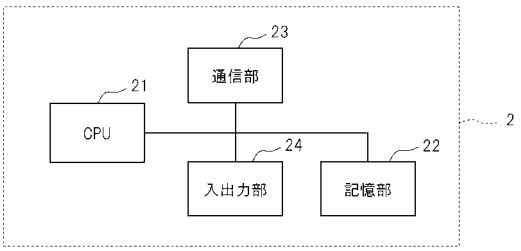
【図１】



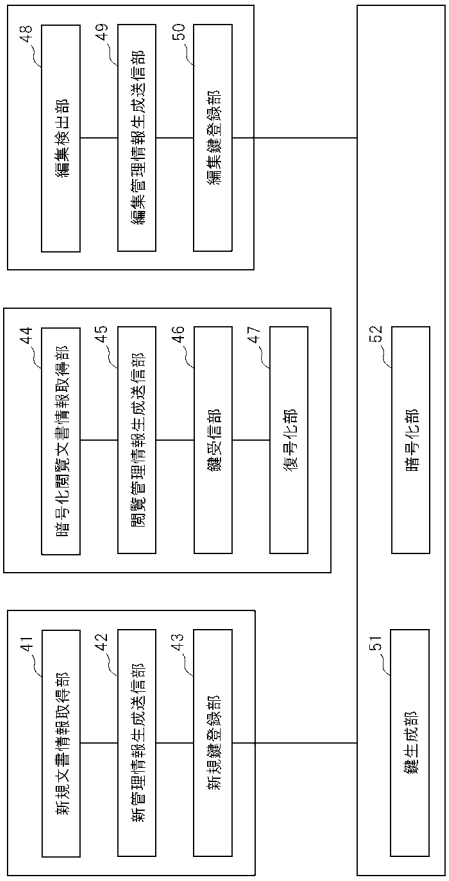
【図２】



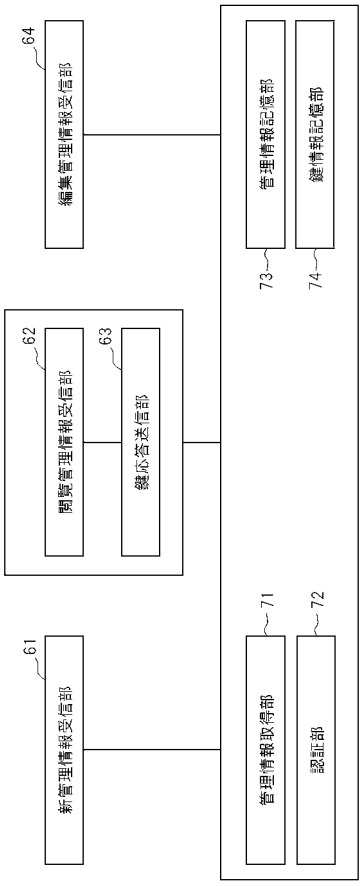
【図３】



【図４】



【図５】



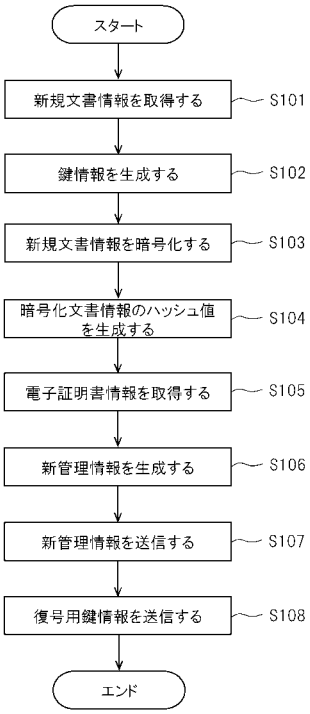
【図６】

	閲覧時	編集時
履歴ID	45c2349a3b84c32	67246b28c6247a8
内容	<user>Alice</user> <timestamp>2007/6/28 10:35</timestamp> <method>閲覧</method> <base></base> <body>3b4d25a2c4b2567813</body> <filename>alpha.doc</filename>	<user>Alice</user> <timestamp>2007/6/30 13:15</timestamp> <method>編集</method> <base>45c2349a3b84c32</base> <body>569845b2a5c613</body> <filename>alpha.doc</filename>

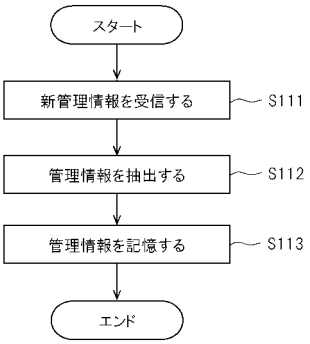
【図７】

	新規作成時
履歴ID	145ca9a161df854
内容	<user>Carol</user> <timestamp>2007/6/27 16:30</timestamp> <method>新規作成</method> <base></base> <body>3b4d25a2c4b2567813</body> <filename>alpha.doc</filename>

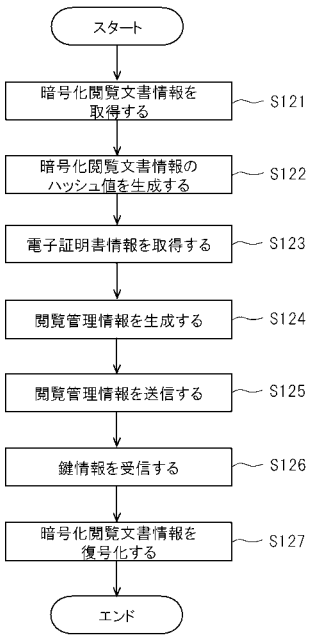
【図８】


スタート
新規文書情報を取得する
S101
鍵情報を生成する
S102
新規文書情報を暗号化する
S103
暗号化文書情報のハッシュ値を生成する
S104
電子証明書情報を取得する
S105
新管理情報を生成する
S106
新管理情報を送信する
S107
復号用鍵情報を送信する
S108
エンド

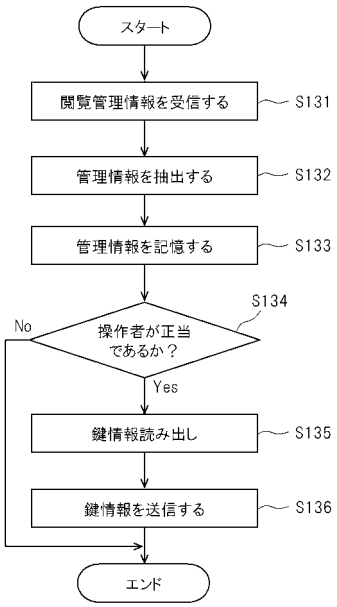
【図９】


スタート
新管理情報を受信する
S111
管理情報を抽出する
S112
管理情報を記憶する
S113
エンド

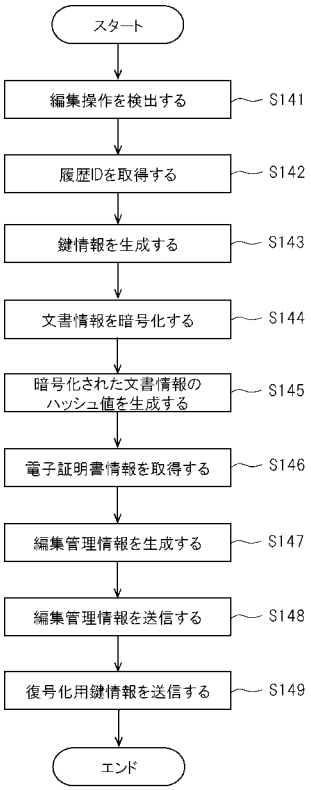
【図１０】


スタート
暗号化閲覧文書情報を取得する
S121
暗号化閲覧文書情報のハッシュ値を生成する
S122
電子証明書情報を取得する
S123
閲覧管理情報を生成する
S124
閲覧管理情報を送信する
S125
鍵情報を受信する
S126
暗号化閲覧文書情報を復号化する
S127
エンド

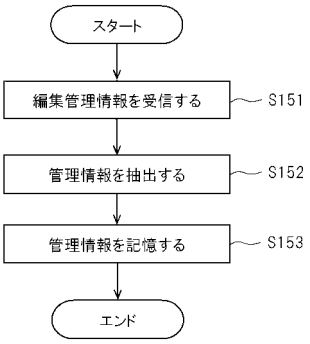
【図１１】


スタート
閲覧管理情報を受信する
S131
管理情報を抽出する
S132
管理情報を記憶する
S133
S134
No
操作者が正当であるか？
Yes
鍵情報読み出し
S135
鍵情報を送信する
S136
エンド

【図１２】



【図１３】



【図１４】

履歴ID	ファイルパス
45c2349a3b84c32	C:¥temp¥test¥data¥alpha.doc
de8933365e16ed3	C:¥temp¥beta.ppt
eeceb5bcf6b4f4d	C:¥test¥2007¥hoge¥pi.xls

【図１５】

コピー前	履歴ID	67246b28c6247a8
	内容	<user>Alice</user> <timestamp>2007/6/30 10:35</timestamp> <method>編集</method> <base>45c2349a3b84c32</base> <body>569845b2a5c613</body> <filename>alpha.doc</filename>
コピー後		9aca89db049dbae <user>Bob</user> <timestamp>2007/6/30 13:15</timestamp> <method>閲覧</method> <base></base> <body>569845b2a5c613</body> <filename>beta.doc</filename>