(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2018-156410
(P2018-156410A)
(43)公開日　平成30年10月4日(2018.10.4)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 17/30	(2006.01)	G06F	17/30	340Z
		G06F	17/30	110C
		G06F	17/30	120A

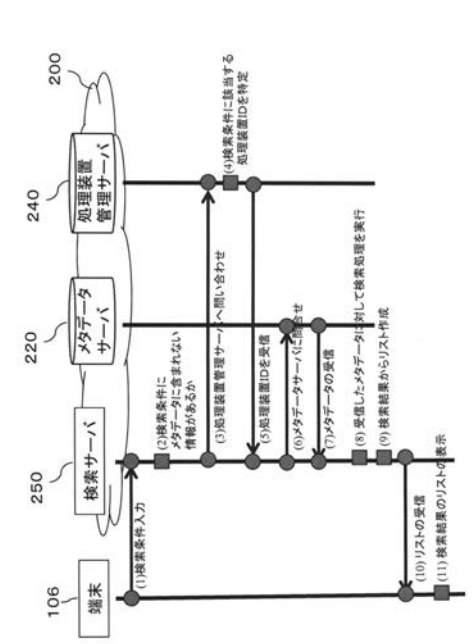
審査請求 未請求　請求項の数 8　ＯＬ　（全 44 頁）

(21)出願番号　特願2017-52851(P2017-52851)
(22)出願日　平成29年3月17日(2017.3.17)

(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　110001210
特許業務法人ＹＫＩ国際特許事務所
(72)発明者　伊與田　哲男
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
(72)発明者　神谷　成樹
東京都港区赤坂九丁目７番３号　富士ゼロックス株式会社内

(54)【発明の名称】情報処理装置及びプログラム

(57)【要約】　（修正有）
【課題】ドキュメントの属性情報にそのドキュメントに関連する主体の属性を含める方式と比べてドキュメントの属性情報のデータ量を抑えつつも、関連する主体の属性でドキュメントを検索する情報処理装置及びプログラムを提供する。
【解決手段】メタデータサーバ２２０には各ドキュメントの属性が記憶され、処理装置管理サーバ２４０には、各ドキュメントを生成した処理装置の属性が記憶されている。検索サーバ２５０は、処理装置の属性に関する第１条件を含む検索条件が入力された場合、その第１条件を満たす処理装置を処理装置管理サーバ２４０に問い合わせ、これに対して回答された処理装置で生成されたドキュメントをメタデータサーバ２２０に問い合わせる。そして、この問合せに対して回答されたドキュメント群から、検索条件のうちの残りの条件を満たすものを検索する。
【選択図】図１９



【特許請求の範囲】
【請求項１】
主体の属性情報に関する検索条件を受け付ける受付手段と、
主体を識別する主体識別情報と前記主体の属性情報とを対応付けて管理する第１管理装置から、前記検索条件を満たす前記属性情報に対応する前記主体識別情報を検索する第１検索手段と、
データと前記データに関連する前記主体の前記主体識別情報とを対応付けて管理する第２管理装置から、前記第１検索手段が検索した前記主体識別情報に対応付けられているデータを検索する第２検索手段と、
を含む情報処理装置。
【請求項２】
前記第１管理装置は、時又は期間に対応付けて、前記時又は期間における前記主体の前記主体識別情報及び前記属性情報を管理しており、
前記第２管理装置は、時又は期間に対応付けて、前記時又は期間における前記データに関連する前記主体の前記主体識別情報を前記データに対応付けて管理しており、
前記第１検索手段は、前記検索条件を満たす前記属性情報に対応する時又は期間と主体識別情報とを検索し、
前記第２検索手段は、前記第１検索手段が検索した前記時又は期間と前記主体識別情報とに対応するデータを検索する、
請求項１に記載の情報処理装置。
【請求項３】
前記データに関連する前記主体は、前記データに対して処理を実行した処理装置であり、
前記情報処理装置は、
前記第２検索手段が検索した前記データに対応付けられている前記主体識別情報に対応する前記処理装置に、そのデータに対して再処理を実行させる制御を行う制御手段、
を更に含む請求項１又は２に記載の情報処理装置。
【請求項４】
前記処理は、暗号化ソフトウエアにより前記データを暗号化することで暗号化されたデータを生成する処理であり、
前記再処理は、前記第２検索手段が検索した前記データを前記暗号化ソフトウエアの最新バージョンにより暗号化し直す処理である、
請求項３に記載の情報処理装置。
【請求項５】
前記データに関連する前記主体は、前記データの配信先のユーザであり、
前記第２管理装置は、前記データに対応付けて、前記データに関連する前記主体の前記主体識別情報として前記データの配信先のユーザのユーザ識別情報を管理すると共に、更に前記データに対して処理を実行した処理装置の装置識別情報を管理しており、
前記情報処理装置は、
前記第２検索手段が検索した前記データに対応付けられている前記装置識別情報に対応する前記処理装置に、そのデータに対して再処理を実行させる制御を行う制御手段、
を更に含む請求項１又は２に記載の情報処理装置。
【請求項６】
前記処理は、前記データの配信先のユーザのユーザ識別情報のリストを含んだメタデータを前記データに関連付ける処理であり、
前記再処理は、前記第２検索手段が検索した前記データに関連付けられた前記メタデータにおける前記リストから、前記第１検索手段が検索したユーザのユーザ識別情報を削除する処理である、
請求項５に記載の情報処理装置。
【請求項７】

前記処理は、前記データに対する前記配信先のユーザのアクセス権限の内容を示す情報を含んだメタデータを前記データに関連付ける処理であり、
前記再処理は、前記第２検索手段が検索した前記データに関連付けられた前記メタデータにおける前記アクセス権限の内容を更新する処理である、
請求項５に記載の情報処理装置。
【請求項８】
コンピュータを、
主体の属性情報に関する検索条件を受け付ける受付手段、
主体を識別する主体識別情報と前記主体の属性情報とを対応付けて管理する第１管理装置から、前記検索条件を満たす前記属性情報に対応する前記主体識別情報を検索する第１検索手段、
データと前記データに関連する前記主体の前記主体識別情報とを対応付けて管理する第２管理装置から、前記第１検索手段が検索した前記主体識別情報に対応付けられているデータを検索する第２検索手段、
として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、情報処理装置及びプログラムに関する。
【背景技術】
【０００２】
特許文献１に開示されたシステムでは、表示装置またはプリンタのあるコンピュータを有する複数のユーザから、文書に対する要求を固有のユーザ識別情報とともに受信する。次に、複数のユーザからの要求を著作権サーバで認証する。次に、著作権サーバは、文書サーバに対し各要求の正しい認証に作用するよう指令する。これに応答して、文書サーバは、認証された各要求に対して、独自に符号化され圧縮され暗号化された文書を作成し、認証された各要求ユーザへの文書を、ネットワークを通じて、認証された各要求ユーザの対応する表示または印刷のエージェントへ転送する。文書は、複数のユーザのそれぞれに対応して独自に符号化される。最後に、各エージェントで文書の復号および圧縮解除を行い、認証された要求ユーザによってエージェントに提供された正しい秘密鍵にのみ応答して文書を利用可能にする。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開平７－２３９８２８号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
データには、そのデータの作成者、そのデータを提供する提供先のユーザ、そのデータを生成した装置等、そのデータに関連するいくつかの主体が存在し得る。データの属性情報に対し、そのデータの作成日や作成者等といったそのデータに固有の属性項目の他に、そのデータに関連する主体の属性（例えばデータを生成した装置のバージョンなど）を組み込んでおけば、目的とするデータを検索する際に、関連する主体の属性で検索することが可能になる。
【０００５】
しかし、関連する主体の属性まで含めてしまうと、データの属性情報のデータ量が膨大になってしまい、保存や転送のコストが増大する。
【０００６】
本発明は、データの属性情報にそのデータに関連する主体の属性を含める方式と比べて

データの属性情報のデータ量を抑えつつも、関連する主体の属性でデータを検索できる仕組みを提供する。

【課題を解決するための手段】

【０００７】

請求項１に係る発明は、主体の属性情報に関する検索条件を受け付ける受付手段と、主体を識別する主体識別情報と前記主体の属性情報とを対応付けて管理する第１管理装置から、前記検索条件を満たす前記属性情報に対応する前記主体識別情報を検索する第１検索手段と、データと前記データに関連する前記主体の前記主体識別情報とを対応付けて管理する第２管理装置から、前記第１検索手段が検索した前記主体識別情報に対応付けられているデータを検索する第２検索手段と、を含む情報処理装置である。

【０００８】

請求項２に係る発明は、前記第１管理装置は、時又は期間に対応付けて、前記時又は期間における前記主体の前記主体識別情報及び前記属性情報を管理しており、前記第２管理装置は、時又は期間に対応付けて、前記時又は期間における前記データに関連する前記主体の前記主体識別情報を前記データに対応付けて管理しており、前記第１検索手段は、前記検索条件を満たす前記属性情報に対応する時又は期間と主体識別情報とを検索し、前記第２検索手段は、前記第１検索手段が検索した前記時又は期間と前記主体識別情報とに対応するデータを検索する、請求項１に記載の情報処理装置である。

【０００９】

請求項３に係る発明は、前記データに関連する前記主体は、前記データに対して処理を実行した処理装置であり、前記情報処理装置は、前記第２検索手段が検索した前記データに対応付けられている前記主体識別情報に対応する前記処理装置に、そのデータに対して再処理を実行させる制御を行う制御手段、を更に含む請求項１又は２に記載の情報処理装置である。

【００１０】

請求項４に係る発明は、前記処理は、暗号化ソフトウエアにより前記データを暗号化することで暗号化されたデータを生成する処理であり、前記再処理は、前記第２検索手段が検索した前記データを前記暗号化ソフトウエアの最新バージョンにより暗号化し直す処理である、請求項３に記載の情報処理装置である。

【００１１】

請求項５に係る発明は、前記データに関連する前記主体は、前記データの配信先のユーザであり、前記第２管理装置は、前記データに対応付けて、前記データに関連する前記主体の前記主体識別情報として前記データの配信先のユーザのユーザ識別情報を管理すると共に、更に前記データに対して処理を実行した処理装置の装置識別情報を管理しており、前記情報処理装置は、前記第２検索手段が検索した前記データに対応付けられている前記装置識別情報に対応する前記処理装置に、そのデータに対して再処理を実行させる制御を行う制御手段、を更に含む請求項１又は２に記載の情報処理装置である。

【００１２】

請求項６に係る発明は、前記処理は、前記データの配信先のユーザのユーザ識別情報のリストを含んだメタデータを前記データに関連付ける処理であり、前記再処理は、前記第２検索手段が検索した前記データに関連付けられた前記メタデータにおける前記リストから、前記第１検索手段が検索したユーザのユーザ識別情報を削除する処理である、請求項５に記載の情報処理装置である。

【００１３】

請求項７に係る発明は、前記処理は、前記データに対する前記配信先のユーザのアクセス権限の内容を示す情報を含んだメタデータを前記データに関連付ける処理であり、前記再処理は、前記第２検索手段が検索した前記データに関連付けられた前記メタデータにおける前記アクセス権限の内容を更新する処理である、請求項５に記載の情報処理装置である。

【００１４】

請求項８に係る発明は、コンピュータを、主体の属性情報に関する検索条件を受け付ける受付手段、主体を識別する主体識別情報と前記主体の属性情報とを対応付けて管理する第１管理装置から、前記検索条件を満たす前記属性情報に対応する前記主体識別情報を検索する第１検索手段、データと前記データに関連する前記主体の前記主体識別情報とを対応付けて管理する第２管理装置から、前記第１検索手段が検索した前記主体識別情報に対応付けられているデータを検索する第２検索手段、として機能させるためのプログラムである。

【発明の効果】

【００１５】

請求項１又は８に係る発明によれば、データの属性情報にそのデータに関連する主体の属性を含める方式と比べてデータの属性情報のデータ量を抑えつつも、関連する主体の属性でデータを検索できる。

【００１６】

請求項２に係る発明によれば、過去のある時又は期間において検索条件を満たす主体に対して、その時又は期間において関連するデータを検索することができる。

【００１７】

請求項３に係る発明によれば、検索条件を満たす主体である処理装置により処理されたデータを検索して、そのデータをその処理装置に再処理させることができる。

【００１８】

請求項４に係る発明によれば、脆弱性のある暗号化ソフトウエアで暗号化されたデータを検索し、最新の脆弱性がない暗号化ソフトウエアで再暗号化することができる。

【００１９】

請求項５に係る発明によれば、検索条件を満たす主体であるユーザに配信されたデータを検索して、そのデータを処理した処理装置にそのデータを再処理させることができる。

【００２０】

請求項６に係る発明によれば、属性が変更されるユーザに配信されたデータについて、そのユーザを配信先から外したい場合に、そのようなユーザに配信されたデータを検索し、そのように配信先の変更を行うことができる。

【００２１】

請求項７に係る発明によれば、属性が変更されるユーザに配信されたデータに対して、その属性変更に伴ってデータに対するアクセス権限を変更したい場合に、そのようなユーザに配信されたデータを検索し、検索したデータに対するアクセス権限の内容を変更することができる。

【図面の簡単な説明】

【００２２】

【図１】ドキュメント管理システムの構成の例を示す図である。

【図２】ドキュメント管理システムを利用したドキュメントの配信及び閲覧の概要を説明するための図である。

【図３】メタデータのデータ内容を例示する図である。

【図４】ユーザＩＤサーバが管理するデータ内容を例示する図である。

【図５】ＤＩＤサーバが管理するデータ内容を例示する図である。

【図６】処理装置管理サーバが管理するデータ内容を例示する図である。

【図７】処理装置の構成及び処理装置が持つデータ内容を例示する図である。

【図８】ドキュメント管理システムにおけるドキュメント配信及び閲覧の流れを説明する図である。

【図９】属性データの入力画面の例を示す図である。

【図１０】オプション設定画面の例を示す図である。

【図１１】リスト画面の例を示す図である。

【図１２】組織内管理システムを設けたシステム構成の例を示す図である。

【図１３】ユーザが自分の登録されていない処理装置を用いてドキュメントのメタデータ

取得及び閲覧を行う際の処理の流れの例を示す図である。
【図１４】ユーザが自分の登録されていない処理装置を用いてドキュメント管理システムにドキュメントを登録する際の処理の流れの例を示す図である。
【図１５】ＤＩＤのデータ内容の例を示す図である。
【図１６】処理装置管理サーバが実行する処理装置のステータスチェック処理の流れを例示する図である。
【図１７】処理装置管理サーバが実行する処理装置のステータスチェック処理の流れの別の例を示す図である。
【図１８】暗号化ソフトに脆弱性が見つかった場合の処理装置の処理の流れを例示する図である。
【図１９】保護済みドキュメントの検索の流れを例示する図である。
【図２０】検索サーバの処理手順を例示する図である。
【図２１】検索サーバの処理手順の別の例を示す図である。
【発明を実施するための形態】
【００２３】
図１に、ドキュメント管理システムの一つの実施形態の概略構成を示す。
【００２４】
紙の文書の場合、文書を持つ者が自由にコピーしたり他人に渡したりすることができる。また、文書を入手した者は、その文書を読むことができる。このように、紙の文書は情報漏洩を招くリスクが極めて高い。
【００２５】
これに対して、本実施形態のドキュメント管理システムは、電子的なドキュメントをセキュアに利用できる環境を提供し、ドキュメントの情報が漏洩するリスクを下げることを目指す。ここで、ドキュメントは、１つの単位（例えば１つのファイル）として流通可能なコンテントデータであり、データの種類は特に限定されない。例えば、ドキュメントの概念には、テキストデータ、ワードプロセッサソフトで作成された文書データ、表計算ソフトで作成されたスプレッドシートデータ、ＣＡＤ（Computer Aided Design）データ、画像データ、動画データ、音声データ、マルチメディアデータ、ウェブブラウザで表示されたページデータ、その他PC上で作成・編集・閲覧されプリントアウト対象となる様なデータなどが含まれる。
【００２６】
このドキュメント管理システムは、複数のローカルシステム１００とそれらローカルシステムに関する管理（特に後述する処理システムの管理）を行う管理システム２００とを含む。管理システム２００は、インターネット等の広域ネットワーク１０を介して各ローカルシステム１００と通信可能である。
【００２７】
ローカルシステム１００は、ローカルネットワーク１０８に接続された１以上の作成端末１０２、１以上の閲覧端末１０４、及び処理装置１１０を含む。ローカルネットワーク１０８は、企業等の組織内に設けられたプライベートネットワーク（例えばＬＡＮとして構成）であり、ファイアウォール等により広域ネットワーク１０から保護されている。処理装置１１０は、基本的に、ローカルシステム１００内に１つ設置される。組織内のプライベートネットワークが大規模なものである場合、プライベートネットワークを構成する個々のネットワークセグメントをそれぞれローカルシステム１００とし、それら個々のローカルシステム１００内に１つずつ処理装置１１０を設置してもよい。例えば、ある会社の部署毎の居室内のネットワークセグメントがそれぞれその部署のローカルシステム１００となり、そのセグメントに１つの処理装置１１０が設置される。この例では、会社毎や各会社の部署毎に処理装置１１０を核とするローカルシステム１００が形成され、それら各処理装置１１０が中央にある管理システム２００から管理される。
【００２８】
作成端末１０２は、ドキュメントを作成するために用いられる端末であり、例えばデス

クトップ型又はノート型のパーソナルコンピュータ、ワークステーション、タブレット端末、スマートフォン、複合機、スキャナ、ファクシミリ装置、デジタルカメラ等がその例である。作成端末１０２には、ドキュメントの作成、編集等のためのアプリケーションがインストールされている。また、作成端末１０２には、作成したドキュメントの配信をドキュメント管理システムに依頼するためのソフトウエアがインストールされている。このソフトウエアの形態としては、後述する処理装置１１０と情報をやりとりするデバイスドライバとして実装、またはＷｅｂアプリによる実装、などが考えられる。

【００２９】

処理装置１１０は、作成端末１０２が作成したドキュメントを、本実施形態のドキュメント管理システムが提供するセキュアな環境で用いる形態である保護済みドキュメント（以下では「ｅＤｏｃファイル」とも呼ぶ）へと変換するという保護処理を実行する。保護処理は、元のドキュメントをｅＤｏｃへとエンコードする処理ともいえ、この意味では処理装置１１０は一種のエンコーダである。この保護処理では、ドキュメントを、例えば、本実施形態のシステムのために設計された専用フォーマットのデータに変換すると共に、そのドキュメントの配信先に指定されたユーザにのみ復号可能な形で暗号化する。フォーマット変換と暗号化はどちらを先に行ってもよい。

【００３０】

また処理装置１１０は、保護済みドキュメントのメタデータを作成し、作成したメタデータを上位システムである管理システム２００に登録する。メタデータは、当該保護済みドキュメントの書誌事項、配信先の情報、各配信先が保護済みドキュメントの暗号化を解除するのに用いるキーの情報等を含む。メタデータは複数の項目を含み、このサービスで提供される機能に応じて対応するデバイスやユーザからデータ付与・編集・更新が実行される。

【００３１】

例として、それら項目のうちの一部を、ドキュメント管理システムに対するドキュメントの登録指示を行ったユーザが指定し、別の一部は処理装置１１０が作成する。また、メタデータのうちの一部の項目の値を管理システム２００や閲覧端末１０４が設定することもあり得る。また、処理装置１１０は、生成した保護済みドキュメント（ｅＤｏｃファイル）を、ユーザの指定した配信先の閲覧端末１０４に送信する。

【００３２】

保護済みドキュメントすなわちｅＤｏｃファイルは、元のドキュメントを専用フォーマットに変換し暗号化したものであり、ｅＤｏｃの本体とも呼ぶ。ｅＤｏｃファイルを閲覧可能とするには、対応するメタデータが必要となる。ｅＤｏｃファイルとメタデータとが揃って、閲覧可能な完全な保護済みドキュメントを構成する。このように、ｅＤｏｃファイルとこれに対応するメタデータとの組を、以下では「ｅＤｏｃ」と呼ぶ。

【００３３】

処理装置１１０は、無線ＬＡＮのアクセスポイントの機能を内蔵していてもよい。この場合、閲覧端末１０４は、無線ＬＡＮで処理装置１１０と通信可能である。

【００３４】

閲覧端末１０４は、保護済みドキュメント（ｅＤｏｃファイル）の閲覧に用いられる端末である。ここで言う「閲覧」は、保護済みドキュメントをそのドキュメントが表す情報内容に応じた態様で利用することを意味する。例えば、保護済みドキュメントがワープロデータや図面等の文書を情報内容として持つ場合、閲覧は、閲覧端末１０４が表示したその文書をユーザが読む又は見ることである。また保護済みドキュメントが表す情報内容が音声である場合、閲覧とは、閲覧端末１０４が再生したその音声をユーザが聞くことである。閲覧端末１０４は、例えば、デスクトップ型又はノート型のパーソナルコンピュータ、ワークステーション、タブレット端末、スマートフォン等の汎用のコンピュータに、保護済みドキュメントを閲覧するためのビューワアプリケーションをインストールして構成される。また、電子書籍端末のような閲覧専用の端末に、ビューワアプリケーションと同等の機能を持たせたものを閲覧端末１０４として用いてもよい。ビューワアプリケーショ

ンは、暗号化されている保護済みドキュメントをメタデータの情報を用いて復号する機能や、保護済みドキュメントの専用フォーマットで表されるデータを可読な状態のデータへとデコードする機能を有する。なお、本実施形態のドキュメント管理システムに対応するビューワアプリケーションを持たないコンピュータは、専用フォーマットのデータを可読なデータへとデコードすることはできない。

【００３５】

閲覧端末１０４は、保護済みドキュメントを復号及びデコードして表示する機能に加え、表示したそのドキュメントに対するユーザからの加工（編集）を受け付ける機能を有していてもよい。加工されたドキュメントは、元の保護済みドキュメントとは異なる内容となるが、この編集後のドキュメントを閲覧端末１０４から処理装置１１０に送ってドキュメント管理システムに登録（すなわち保護済みドキュメントへとエンコード）できるようにしてもよい。このように、１つの端末が、作成端末１０２と閲覧端末１０４の両方の機能を持っていてもよい。なお、ｅＤｏｃには閲覧者に許可する権限（後述するメタデータ中のアクセス権限情報）が設定されており、その権限の内容には、そのｅＤｏｃへの書き込み制限、再配布先の制限などが含まれてもよい。このような制限がアクセス権限情報中に規定されているｅＤｏｃの場合、閲覧端末１０４は、閲覧者からの加工（編集）操作をその書き込み制限の範囲内でのみ受け付け、また加工後の新たなｅＤｏｃの再配布先の指定を、その再配布先の制限の範囲内でのみ受け付ける。

【００３６】

また、本実施形態では、一例として、本実施形態のドキュメント管理システムを利用するユーザを認証するためのツールとして、ユーザが携帯する認証デバイス１３０を用いる。認証デバイス１３０は、ＩＣカードのように、当該デバイスを携帯するユーザに固有の識別情報を内蔵し、外部装置からの要求に応じてユーザ認証のためのデータ処理を実行するデバイスである。認証デバイス１３０は、そのような個人認証用のＩＣカードと同等の機能を内蔵したスマートフォンのような携帯端末であってもよい。閲覧端末１０４や作成端末１０２は、ＮＦＣ（Near Field Communication）等の無線通信プロトコルを用いて認証デバイス１３０と通信する機能を備える。閲覧端末１０４や作成端末１０２は、認証デバイス１３０との間で所定のプロトコルに沿ってユーザ認証のための情報をやりとりし、その認証デバイス１３０を携帯するユーザを認証する。あるいは、実際のユーザ認証は処理装置１１０や管理システム２００等、本実施形態のドキュメント管理システムのサーバ側が実行し、閲覧端末１０４や作成端末１０２は、サーバ側と認証デバイス１３０との間のデータ転送の仲介を行う方式であってもよい。また、閲覧端末１０４や作成端末１０２が認証デバイス１３０の機能を内蔵していてもよい。

【００３７】

管理システム２００は、各ローカルシステム１００内の処理装置１１０を管理する。また管理システム２００は、それら各処理装置１１０が生成した保護済みドキュメントのメタデータを管理し、要求に応じてメタデータを閲覧端末１０４に提供する。管理システム２００は、１台のコンピュータ、又は相互に通信可能な複数のコンピュータにより構成され、ユーザＩＤサーバ２１０、ＤＩＤサーバ２２０、メタデータサーバ２３０、処理装置管理サーバ２４０の機能を有する。

【００３８】

ユーザＩＤサーバ２１０は、ドキュメント管理システムを利用する各ユーザの情報を管理するサーバである。ドキュメント管理システムを利用するユーザには、２つの階層がある。１つは、ドキュメント管理システムの利用のための契約を本システムの運営者と結んだ契約者であり、もう１つはその契約の下で実際にシステムを利用してドキュメントの登録や閲覧を行う一般ユーザである。例えば、会社が契約者であり、その会社のローカルネットワーク１０８に処理装置１１０が設置され、その会社の社員が一般ユーザとして、その処理装置１１０を介してドキュメント管理システムを利用するケースが多いと想定される。ユーザＩＤサーバ２１０は、契約者と一般ユーザのそれぞれについての情報を保持し、管理する。

【００３９】
ＤＩＤサーバ２２０は、保護済みドキュメントの識別情報（ＩＤ）であるＤＩＤ（ドキュメントＩＤ）を管理する。実際に保護済みドキュメントにＤＩＤを付与するのはその保護済みドキュメントを作成した処理装置１１０であるが、ＤＩＤサーバ２２０は処理装置１１０に対してＤＩＤの発行権限と発行枠（発行数）を付与し、その発行権限と発行枠の中で処理装置１１０が実際に発行したＤＩＤの報告を受けて記録する。これにより、ＤＩＤサーバ２２０は、不正なＤＩＤの発生を抑止し、不正なＤＩＤを持つドキュメントを検知可能とする。
【００４０】
メタデータサーバ２３０は、処理装置１１０が生成した保護済みドキュメント（ｅＤｏｃファイル）のメタデータを保持し、管理する。メタデータサーバ２３０は、ユーザから閲覧端末１０４を介して保護済みドキュメントのメタデータを要求された場合、そのユーザが正当な者であれば、メタデータをその閲覧端末１０４に提供する。なお、メタデータを要求するユーザ（閲覧者）がメタデータサーバ２３０にとって「正当な者」であるとは、そのユーザと、そのユーザがその要求を発する際に用いた閲覧端末１０４との組合せが、そのｅＤｏｃファイルのＤＩＤ（これはその要求に含まれる）に対応づけてメタデータサーバ２３０が保持しているメタデータ中の配信先情報（詳しくは後述）に示される配信先ユーザ及び配信先の閲覧端末１０４の組合せに該当する場合のことである。
【００４１】
処理装置管理サーバ２４０は、各処理装置１１０のステータス（状態）を管理するサーバである。
【００４２】
図２を参照して、本実施形態の仕組みを概略的に説明する。
【００４３】
（０）管理システム２００（ＤＩＤサーバ２２０）は、ローカルシステム１００内の処理装置１１０に対してＤＩＤ（ドキュメントＩＤ）の発行権及びこれに付随する発行枠（ドキュメント数）を事前に付与している。ＤＩＤの発行権は、無制限ではなく、管理システム２００の発行枠に制限される。すなわち、処理装置１１０は、管理システム２００から付与された発行枠が示す数までのドキュメントであれば、同時に付与された発行権に基づいたＤＩＤを付与することができる。発行枠を使い切れば、処理装置１１０は、管理システム２００から新たな発行権及び発行枠の付与を受ける。
【００４４】
（１）ユーザは、ドキュメントを本実施形態のドキュメント管理システムに登録したい（すなわち配信したい）場合、作成端末１０２にドキュメント登録を指示する（例えばアプリケーションのメニュー上で「登録」を指示する）。この指示を受けた作成端末１０２は、ユーザ認証を求める。この認証は、ユーザＩＤ及びパスワードの入力により行ってもよいし、作成端末１０２のカードリーダ部の近傍にユーザが認証デバイス１３０を近づけることで行ってもよい。ユーザ認証は、作成端末１０２が行ってもよいし、ドキュメントの登録先である処理装置１１０が行ってもよい。そして、ユーザは、作成端末１０２に保持されているドキュメントからドキュメント管理システムに登録するものを選んでその登録を指示する。
【００４５】
作成端末１０２（より詳しくは、作成端末１０２にインストールされた登録処理用プログラム）は、ユーザからドキュメントの登録指示を受けた場合、そのドキュメントに対する属性データのうちそのユーザが指定すべき項目（例えばドキュメントの配信先）の入力を受け付ける。ここで、配信先として、ユーザと閲覧端末１０４の組合せの指定を受け付けるようにしてもよい。この場合、ユーザと、そのユーザがドキュメントの閲覧に用いる閲覧端末１０４との組合せが、配信先として指定された組合せと一致する場合に、ユーザはそのドキュメントを閲覧可能となる。
【００４６】

作成端末１０２は、ユーザが入力した配信先等の属性項目と、作成端末１０２自身が生成した他の属性項目（例えば登録者の情報、作成日時等）と合わせた属性データを、そのドキュメントのデータと共に処理装置１１０に送信する。なお、作成端末１０２は、様々なアプリケーションが作成した様々なフォーマットのドキュメントを、閲覧端末１０４側で取扱可能な統一的なフォーマットに変換するドライバを有していてもよい。例えば、ワープロデータ、スプレッドシート、ＣＡＤデータのような静的な文書画像を示すデータの場合、そのドライバは、プリンタドライバと同様、そのデータをページ記述言語で表現されたドキュメントへと変換する。また、例えば、元のデータが音声データの場合、ドライバは、その音声データを本実施形態のドキュメント管理システム（特に閲覧端末１０４）が対応する特定の音声データ形式のデータ（ドキュメント）へと変換する。

【００４７】

（２）処理装置１１０は、作成端末１０２から受信した登録対象のドキュメントに対して保護処理を施すことで保護済みドキュメント（ｅＤｏｃファイル）を生成する。この生成では、受信したドキュメントを本実施形態のドキュメント管理システムの専用フォーマットへとエンコードし、エンコードしたデータを、生成した暗号鍵を用いて暗号化することで、ｅＤｏｃファイルを生成する。エンコードと暗号化の順序は逆でもよい。また処理装置１１０は、そのｅＤｏｃに対して一意なＤＩＤを付与する。このＤＩＤには、管理システム２００から受けた発行権限に基づくものであることを証する情報（後述する発行権限キー）と、その処理装置１１０自身が付与したものであることを証する情報（後述する発行証明キー）が含まれる。なお、ＤＩＤのデータ構造については、後で詳細な例を説明する。生成されたＤＩＤは、ｅＤｏｃファイル内に（例えばそのファイルのプロパティの一項目として）組み込まれる。

【００４８】

また処理装置１１０は、生成したｅＤｏｃファイルに対応するメタデータを生成する。このメタデータには、作成端末１０２からそのドキュメントと共に受け取った属性データと、処理装置１１０自身が生成した属性項目（例えば、ＤＩＤ、処理装置自身のＩＤ、エンコード日時、暗号鍵情報）の値とが含まれる。メタデータに含まれる暗号鍵情報は、ｅＤｏｃファイルの暗号化を解除するための鍵を示す情報である。暗号化に共通鍵方式を用いた場合、暗号鍵情報はその共通鍵を示す情報である。ただし、共通鍵そのものを平文でメタデータに含めると、盗聴や傍受により悪用される懸念があるので、その共通鍵を配信先ユーザの公開鍵で暗号化したものを暗号鍵情報としてメタデータに組み込む。

【００４９】

また、処理装置１１０は、生成したｅＤｏｃファイルとメタデータを、内蔵するデータベースに保存する。

【００５０】

（３）処理装置１１０は、生成したメタデータを管理システム２００に送信して登録する。管理システム２００（メタデータサーバ２３０）は、受信したメタデータを保存する。

【００５１】

（４）処理装置１１０は、生成したｅＤｏｃファイルを、配信先に指定された閲覧端末１０４に配信する。この配信は、プッシュ型でもプル型でも、それら両方（例えばｅＤｏｃ作成時にプッシュ配信し、そのときに非稼働で受信しなかった閲覧端末１０４はプル型で配信を受ける）であってもよい。この配信は、ローカルシステム１００内のローカルネットワーク１０８を介して行われる。

【００５２】

（５）閲覧端末１０４が受信したｅＤｏｃファイルは、暗号化等により保護されているのでそのままでは閲覧が不可能である。ユーザは、閲覧端末１０４でそのｅＤｏｃファイルを閲覧したい場合、自分の認証デバイス１３０をその閲覧端末１０４のカードリーダ部に近づけてユーザ認証を受けた後、閲覧端末１０４の画面上でそのｅＤｏｃの閲覧を指示する。この指示を受けた閲覧端末１０４は、管理システム２００にアクセスしてそのｅＤ

ｏｃのメタデータを要求する。この要求には、そのｅＤｏｃのＤＩＤが含まれる。
【００５３】
（６）管理システム２００（メタデータサーバ２３０）は、閲覧端末１０４から要求されたｅＤｏｃの最新のメタデータをその閲覧端末１０４に送信する。
【００５４】
（７）閲覧端末１０４は、要求したメタデータを管理システム２００から受信すると、そのメタデータに含まれる配信先情報に、当該閲覧端末１０４と現在この閲覧端末１０４を利用しているユーザ（認証デバイス１３０で認証済み）との組合せが含まれるかどうかを判定する。含まれていない場合、そのユーザはその閲覧端末１０４でそのｅＤｏｃを閲覧する権限がないので、閲覧端末１０４はｅＤｏｃファイルを開かず、閲覧権限がない旨を示すエラーメッセージを表示する。含まれる場合は、そのユーザはその閲覧端末１０４でそのｅＤｏｃファイルを閲覧する権限を持つ。この場合閲覧端末１０４は、そのｅＤｏｃファイルをそのメタデータに含まれる暗号鍵情報を用いて復号し、画面に表示する（すなわちそのｅＤｏｃファイルの情報内容に応じた態様で出力する）。
【００５５】
メタデータには有効期限を設定する事が出来る。有効期限は、例えばメタデータが送信された日時に対し、規定の有効期間、または配信者等が指定した有効期間を足すことで求められる。閲覧端末１０４は、メタデータの有効期限が過ぎた後には、メタデータを再度管理システム２００から取得し直さないと、対応するｅＤｏｃファイルを開く（復号及び表示する）ことができない。閲覧端末１０４は、処理装置１１０又は管理システム２００と通信可能であれば、閲覧対象に指示されたｅＤｏｃファイルのその指示の時点での最新のメタデータを処理装置１１０又は管理システム２００から取得し、この最新のメタデータに基づいて閲覧可否を判定する。
【００５６】
メタデータが最初の管理システム２００に登録された後、そのメタデータに含まれる配信先情報やアクセス権限情報が配信者、または配信先の変更権限が与えられた者（例えばデータの編集権限を保有する者）により変更されることがある。ｅＤｏｃが作成・登録された時点で配信先に指定されたユーザであっても、その後の変更により配信先から外された場合には、閲覧端末１０４は、管理システム２００から取得した最新のメタデータに含まれる配信先情報によりそのことを検知し、ｅＤｏｃファイルの表示を行わない。
【００５７】
次に、図３を参照して、ｅＤｏｃのメタデータ３００のデータ内容の例を説明する。
【００５８】
メタデータ３００の含む項目のうち、まず「ＤＩＤ」は、そのｅＤｏｃを生成した処理装置１１０が付与したドキュメントＩＤである。「ドキュメント名」は、そのｅＤｏｃの名称又はタイトルである。
【００５９】
「配信者ＩＤ」は、そのｅＤｏｃを配信した者、すなわち作成端末１０２から処理装置１１０に対してドキュメントの登録操作を行い、処理装置１１０を介して配信を行う者（以下、配信者と呼ぶ）のユーザＩＤである。
【００６０】
「エンコード日時」は、作成端末１０２からのドキュメントがエンコード（保護処理）されてそのｅＤｏｃが作成された日時である。「処理装置ＩＤ」は、その保護処理を実行した処理装置の識別情報である。「暗号化情報」は、そのｅＤｏｃの生成時の暗号化に関する情報であり、暗号化に用いた暗号化ソフト名、その暗号化ソフトのバージョン、及びその暗号化を解除（復号）するための鍵を表す鍵情報を含む。鍵情報は、例えば、復号のための鍵を各配信先ユーザの公開鍵で暗号化したものである。「キーワード情報」は、そのｅＤｏｃ（又は元データ）から抽出したキーワードのリストである。このキーワード情報は、例えばｅＤｏｃの検索の際に利用される。
【００６１】

「配信先情報」は、配信者がそのｅＤｏｃの配信先に指定したユーザ及び閲覧端末を表す情報である。図３の例では、配信先情報は、配信先のユーザ毎に、そのユーザのユーザＩＤとそのユーザが閲覧に用いるべき閲覧端末１０４のＩＤ（識別情報）とを含んでいる。そのユーザがそのｅＤｏｃの閲覧に利用可能な閲覧端末１０４が複数指定された場合は、そのユーザのユーザＩＤとそれら複数の閲覧端末１０４のＩＤとの組が配信先情報に組み込まれる。

【００６２】

また別の例として、配信先ユーザは配信先に指定された閲覧端末１０４のうちのいずれを利用してもそのｅＤｏｃを閲覧可能とする方式を採用した場合、配信先情報には、配信先ユーザのＩＤのリストと、配信先の閲覧端末１０４のＩＤのリストが含まれる。例えば、配信先の閲覧端末１０４の候補として、部署の共用端末や、部署の居室や会議室に備え付けられた端末等が想定される場合がある。共用端末や居室等の備え付け端末（これも共用端末の一種）等は、組織内のユーザのだれが使うか決まっていないが、少なくともどのような端末であるかは配信者には分かっており、また勝手に組織外に持ち出される可能性が低いことも分かっているので、機密対象のドキュメントの配信先として適格である。このように素性の分かった共用端末でｅＤｏｃを利用する場合には、このように配信先ユーザは配信先に指定された閲覧端末１０４のうちのどれを利用してもよい、という利用形態も考えられる。

【００６３】

「アクセス権限情報」は、配信者が配信先のユーザに対して付与したそのｅＤｏｃに対する利用権限を表す情報である。

【００６４】

「オフライン有効期間」は、そのメタデータの有効期間の長さを表す情報である。すなわち、閲覧端末１０４が管理システム２００にアクセスできない状態（オフライン状態）にあるときでも、そのｅＤｏｃの前回の閲覧時に取得してキャッシュしているメタデータが存在し、そのメタデータの取得日時からその「オフライン有効期間」内であれば、閲覧端末１０４はそのメタデータ内の暗号鍵情報を用いてそのｅＤｏｃを復号して表示する。一方、オフライン状態であり、閲覧を指示されたｅＤｏｃについてのキャッシュしたメタデータのオフライン有効期間が既に過ぎている場合は、閲覧端末１０４は、そのｅＤｏｃを復号せず、したがって表示も行わない。なお、閲覧端末１０４は、管理システム２００にアクセス可能（すなわちオンライン状態）である間は、ユーザがｅＤｏｃの閲覧を指示した場合、そのｅＤｏｃの最新のメタデータを管理システム２００（特にメタデータサーバ２３０）から取得して使用する。

【００６５】

「元データ情報」は、ｅＤｏｃが生成（エンコード）される前の元データが保存されているか否かを示す情報と、保存されている場合はその元データの保存場所を示す情報（例えばＵＲＬ：Uniform Resource Locator）である。ここでの元データは、例えば作成端末１０２から処理装置１１０に送られたドキュメント（保護処理を施す前のもの）、又はそのドキュメントの元になったアプリケーションデータ（例えばドキュメントがページ記述言語データである場合、そのデータに変換する前のワープロソフトのデータ）、又はそれらの両方である。

【００６６】

「ドキュメント取得日時」は、閲覧端末１０４がそのｅＤｏｃの本体データのファイル（すなわちｅＤｏｃファイル）を取得した日時である。「メタデータ取得日時」は、閲覧端末１０４がそのｅＤｏｃの現在キャッシュしている最新のメタデータを管理システム２００から取得した日時である。ドキュメント取得日時及びメタデータ取得日時は、管理システム２００に保持されているメタデータには含まれず、閲覧端末１０４が管理システム２００から取得したメタデータに対して自機での管理のために追加する。

【００６７】

また図３に示したメタデータの項目のうち、ＤＩＤ、エンコード日時、処理装置ＩＤ、

暗号化情報、キーワード情報は、処理装置１１０が生成する情報である。また、ドキュメント名、配信者ＩＤ、配信先情報、アクセス権限情報、オフライン有効期間、元データ情報は、作成端末１０２から処理装置１１０に送られるドキュメントや属性データに由来する。

【００６８】

次に、管理システム２００の各サーバ２１０～２５０が管理する情報のデータ内容を例示する。

【００６９】

まず図４を参照して、ユーザＩＤサーバ２１０が管理するデータ内容の例を説明する。ユーザＩＤサーバ２１０には、各契約者の契約者データ２１２と、各一般ユーザのユーザデータ２１４が登録されている。

【００７０】

契約者データ２１２には、契約者ＩＤ、契約内容情報、及びユーザリストが含まれる。契約者ＩＤは、ドキュメント管理システムの運営者と契約した契約者（例えば組織や組織内の部署）の識別情報である。ユーザリストは、その契約者の契約によってこのドキュメント管理システムを利用する一般ユーザ（例えば契約者である組織に所属するメンバ）のユーザＩＤのリストである。

【００７１】

一般ユーザデータ２１４には、その一般ユーザのユーザＩＤ、パスワード、ユーザＩＤキー情報、公開鍵証明書、既定の処理装置ＩＤ、既定の閲覧端末リスト、所属情報を含む。ユーザＩＤキー情報は、そのユーザの認証デバイス１３０が用いるそのユーザの認証情報である。公開鍵証明書は、そのユーザの公開鍵を証明するデジタル証明書である。既定の処理装置ＩＤは、そのユーザが登録された処理装置１１０のＩＤである。通常、ユーザは自分が所属するオフィスに置かれた処理装置１１０に登録され、その処理装置１１０がそのユーザにとっての既定の処理装置となる。既定の閲覧端末リストは、そのユーザが主として使用する１以上の閲覧端末のＩＤのリストである。このリストに含まれる閲覧端末が、そのユーザに対してｅＤｏｃを配信する際の配信先の端末の候補となる。所属情報は、そのユーザが所属する組織やその部署等を特定する情報であり、例えばその組織や部署の契約者ＩＤである。

【００７２】

次に図５を参照して、ＤＩＤサーバ２２０が管理するデータ内容の例を示す。

【００７３】

ＤＩＤサーバ２２０は、図５に示すように、処理装置に対して発行した発行権限キー毎に、発行枠、付与先処理装置、キー付与日時、キー終了日時、発行済ＤＩＤリストの各項目の情報を保持している。

【００７４】

発行権限キーは、ＤＩＤサーバ２２０が処理装置１１０に対して付与した、ＤＩＤの発行権限を証明するキー情報（例えばランダムに生成した文字列）である。処理装置１１０は、自らが発行するＤＩＤに、ＤＩＤサーバ２２０から付与された発行権限キーを含めることで、そのＤＩＤが正当な発行権限の下で発行したものであることを証する。

【００７５】

発行枠は、その発行権限キーと共に処理装置１１０に付与したＤＩＤ発行上限数（ＤＩＤを付与可能な上限のドキュメント数）である。処理装置１１０は、発行権限キーと発行枠のペアをＤＩＤサーバ２２０から付与されると、その発行枠が示す上限数までのｅＤｏｃに対して、それぞれ固有のＤＩＤを付与することができる。

【００７６】

付与先処理装置は、その発行権限キー（及び発行枠）の付与先の処理装置１１０のＩＤを示す。キー付与日時は、その発行権限キーを処理装置１１０に付与した日時である。キー終了日時は、付与先の処理装置１１０がその発行権限キーを使い終わった日時である。すなわち、処理装置１１０がその発行権限キーと共に付与された発行枠が示す上限数のｅ

Ｄｏｃに対するＤＩＤの付与をし終えた日時である。なお、処理装置１１０が発行枠を使い切った後に次の発行権限キーと発行枠をＤＩＤサーバ２２０に要求する仕組みを採用している場合、ある発行権限キー（第１のキーと呼ぶ）のキー終了日時を明示的に記録する代わりに、当該発行権限キーの次に処理装置１１０が付与された発行権限キーのキー付与日時を、第１のキーのキー終了日時として用いてもよい。発行済ＤＩＤリストは、付与先の処理装置１１０がその発行権限キーを用いて発行したＤＩＤとその発行年月日のリストである。付与先の処理装置１１０は、発行権限キーを用いてＤＩＤを発行する毎にそのＤＩＤをＤＩＤサーバ２２０に通知し、ＤＩＤサーバ２２０は通知されたＤＩＤとその発行年月日を、そのＤＩＤに含まれる発行権限キーに対応する発行済ＤＩＤリストに追加する。

【００７７】

メタデータサーバ２３０は、各処理装置１１０から送られてくる各ｅＤｏｃのメタデータを保管する。保管するメタデータのデータ内容は、図３に例示したものと同様である。ただし、図３に例示したメタデータの項目のうち、閲覧端末１０４のみで用いる項目（ドキュメント取得日時やメタデータ取得日時等）については、メタデータサーバ２３０では管理しない。

【００７８】

次に図６を参照して処理装置管理サーバ２４０が管理するデータについて説明する。処理装置管理サーバ２４０は、管理対象の処理装置１１０毎に、その処理装置１１０のステータス履歴２４２を記憶している。ステータス履歴には、その処理装置１１０のＩＤに対応付けて、作成及び個々の更新の時点（作成・更新日時）でのその処理装置１１０のステータス２４４の情報が含まれる。

【００７９】

個々の時点でのステータス２４４には、設置場所、契約者ＩＤ、管理者名、管理者連絡先、登録ユーザリスト、ソフトウエア情報２４６、ハードウエア情報２４８、ディスク空き容量、セキュリティ証明書情報が含まれる。設置場所は、その処理装置１１０の設置場所を示す情報であり、例えば住所や建物名、階数などの情報を含む。契約者ＩＤは、その処理装置１１０を使用している契約者のＩＤである。管理者名は、その処理装置１１０の管理者の名前である。管理者は、処理装置１１０の設置先の部署等においてその処理装置１１０を管理しているユーザである。管理者連絡先は、その管理者の連絡先の情報（例えば電子メールアドレス）である。登録ユーザリストは、その処理装置１１０に登録されたユーザ（言い換えればその処理装置１１０を「既定の処理装置」とするユーザ）のユーザＩＤのリストである。

【００８０】

ソフトウエア情報２４６には、エンコードソフト名、エンコードソフトバージョン、暗号化ソフト名、暗号化ソフトバージョン、処理装置１１０にインストールされているその他のソフトウエアの名称及びバージョンが含まれる。ここでエンコードソフトは、作成端末１０２から入力されたドキュメントを、ドキュメント管理システムの専用フォーマットへと変換（エンコード）するソフトウエアである。暗号化ソフトは、ドキュメント（例えば専用フォーマットに変換されたもの）を暗号化するソフトウエアである。

【００８１】

ハードウエア情報２４８には、エンコード回路情報、エンコード回路ＦＷバージョン、当該処理装置１１０の製造者名等の項目が含まれる。エンコード回路情報は、エンコード処理に用いるハードウエア回路の機種を示す情報である。エンコード回路ＦＷバージョンは、そのエンコード回路のファームウェア（ＦＷ）のバージョンである。

【００８２】

ディスク空き容量は、処理装置１１０が持つハードディスク又はソリッドステートディスク等の二次記憶装置の、その時点での空き容量である。

【００８３】

セキュリティ証明書情報は、処理装置１１０にその時点でインストールされている各セ

キュリティ証明書を特定する情報（例えば証明書のサブジェクト（subject:主体者）識別子、イシュア（issuer:発行者）識別子、発行日時等の情報）である。

【００８４】

また煩雑さを避けるために図示は省略したが、ステータス２４４には、処理装置１１０にインストールされているフォントの種類（フォント名のリスト）、ネットワーク通信のためのアドレス（例えばＩＰアドレス）、搭載している二次記憶装置（ハードディスクドライブ等）の装置ＩＤ、処理装置１１０を設置先の組織の基幹システムの処理に繋ぐためのカスタマイズ内容を示す情報、処理装置１１０が用いる暗号鍵（通信路暗号化や署名等のためのもの）のインストール日時等が含まれる。

【００８５】

次に図７を参照して、処理装置１１０が保持するデータベース群について説明する。図示のように、処理装置１１０は、管理情報記憶部１１２、ユーザＤＢ１１４及びドキュメントＤＢ１１６を含む。

【００８６】

管理情報記憶部１１２には、管理情報１１２ａが記憶される。管理情報１１２ａには、上位装置アドレス情報、セキュリティ証明書、暗号鍵、エンコードソフト名、エンコードソフトバージョン、暗号化ソフト名、暗号化ソフトバージョン等の項目が含まれる。上位装置アドレス情報は、処理装置１１０を管理する上位装置のそれぞれの通信アドレス（例えばＩＰアドレス、ＵＲＬ等）の情報である。管理システム２００やその中の各サーバ２１０～２４０、又は後述する組織内管理システム１５０やその中の各サーバ１５２～１５６が上位装置の例である。セキュリティ証明書は、処理装置１１０がネットワーク上の他の装置と公開鍵基盤準拠のセキュアな通信を行う際に用いるデジタル証明書である。処理装置１１０は、よく通信する相手である各上位装置のセキュリティ証明書を保持している。また作成端末１０２や閲覧端末１０４を使用する各ユーザのセキュリティ証明を保持してもよい。暗号鍵は、処理装置１１０がネットワーク上の他の装置と通信を行う際の暗号化や復号、処理装置１１０によるデジタル署名（又はそれに類する証明情報の生成）等の目的に用いる、当該処理装置１１０の暗号鍵であり、例えば公開鍵基盤においてその処理装置１１０に対して付与された秘密鍵と公開鍵のペアである。エンコードソフト及び暗号化ソフトは、それぞれ、この処理装置１１０にインストールされているエンコード（専用フォーマットへの変換）及び暗号化のためのソフトウエアである。

【００８７】

ユーザＤＢ１１４には、この処理装置１１０に登録されている各ユーザ（言い換えればこの処理装置１１０を「既定の処理装置」とするユーザ）のユーザ情報１１４ａが記憶されている。個々の登録ユーザのユーザ情報１１４ａには、ユーザＩＤ、パスワード、ユーザＩＤキー情報、公開鍵情報、既定の閲覧端末リスト等の項目が含まれる。これらの項目については、上述のユーザＩＤサーバ２１０が持つデータの説明（図４参照）で説明した。

【００８８】

ドキュメントＤＢ１１６には、処理装置１１０が生成したｅＤｏｃファイルと、そのｅＤｏｃファイルに対応するメタデータとが保存される。ｅＤｏｃファイルとメタデータとはＤＩＤの情報を含んでいるので、対応付けが可能である。またドキュメントＤＢ１１６には、ｅＤｏｃにエンコードする前の元のデータ（作成端末１０２から受け取ったもの）を、そのｅＤｏｃのＤＩＤに対応付けて登録してもよい。

【００８９】

作成端末１０２及び閲覧端末１０４は、当該端末を利用するユーザ毎に、そのユーザの認証情報（ユーザＩＤ、パスワード等）、既定の処理装置のＩＤ、既定の処理装置のアドレス情報、上位装置（例えば管理システム２００や後述の組織内管理システム１５０）のアドレス情報、処理装置や上位装置のセキュリティ証明書、通信路暗号化等に用いる暗号鍵等を記憶している。

【００９０】

＜システムの処理の流れ＞
ローカルネットワーク１０８上に処理装置１１０を設置した場合、処理装置１１０の保守を行う保守作業員は、処理装置１１０に対して、その処理装置１１０を利用するユーザの情報や、それらユーザが利用する可能性のある作成端末１０２や閲覧端末１０４の情報を登録する。登録されたユーザの情報は、上位装置であるユーザＩＤサーバ２１０（あるいは後述のローカルユーザＩＤサーバ１５２）にも転送され、登録される。なお、設置後、処理装置１１０を利用するユーザが増えたり減ったりした場合には、保守作業員は、処理装置１１０に対して増えたユーザの情報を新たに追加登録したり、減ったユーザの情報の登録を削除したりする作業を行う。このような追加や削除は、ユーザＩＤサーバ２１０等の上位装置にも通知され、これに応じ上位装置の保持する情報が更新される。また保守作業員は、それら各作成端末１０２に対して、処理装置１１０にドキュメントの登録及び配信を依頼する処理を行うソフトウエア（例えば処理装置１１０のデバイスドライバの形態をとる）をインストールする。また、保守作業員は、各閲覧端末１０４に対して、処理装置１１０と通信するための情報（例えば装置名、通信アドレス、無線アクセス設定）等を登録する。
【００９１】
次に図８を参照して、本実施形態のドキュメント管理システムを経由してドキュメントが登録及び配信される際の処理の流れを説明する。
【００９２】
（１）－１：　ユーザ（配信者）が作成端末１０２に対してドキュメントの登録の指示を行うと、作成端末１０２は、ログイン認証情報（例えばユーザＩＤ及びパスワード、又は認証デバイス１３０）の入力を求める画面を表示する。配信者がその求めに応じて認証情報を入力すると、作成端末１０２は、その認証情報をローカルネットワーク１０８経由で処理装置１１０に送信する。
【００９３】
（１）－２：　ログイン認証情報を受け取った処理装置１１０はその情報を用いてユーザ認証を行う。ここではそのユーザ認証が成功した（正しいユーザと確認できた）とする。図示例では、ログインＩＤとパスワードを用いてログイン認証を行っているが、作成端末１０２が認証デバイス１３０との通信に対応している場合は認証デバイス１３０を用いてログイン認証を行ってもよい。
【００９４】
（２）－１：　ログイン認証が成功すると、ユーザは、作成端末１０２に保持されたドキュメントの中からドキュメント管理システムに登録したい（そして他のユーザに配信したい）ドキュメントを選択し、処理装置１１０への登録を指示する。すると、処理装置１１０とのインタフェースとなるソフト（例えばデバイスドライバ）が起動し、ユーザからそのドキュメントについての属性データの入力を受け付け、受け付けた属性データとそのドキュメントのデータを処理装置１１０に送信する。
【００９５】
図９に、この属性データの入力画面４００の一例を示す。この入力画面４００は、配信先ユーザ選択メニュー４０２、配信先ユーザリスト欄４０４、配信先端末選択メニュー４０６、配信先端末リスト欄４０８、アクセス権限設定欄４１０、オフライン有効期間メニュー４１２、及びオプション設定呼出ボタン４１４を含む。
【００９６】
配信先ユーザ選択メニュー４０２は、そのドキュメントの配信先ユーザの選択肢を列挙するプルダウン形式のメニューである。選択肢となるユーザは処理装置１１０に登録されたユーザであり、選択肢となるそれらユーザのＩＤ及びユーザ名のリストは処理装置１１０から取得すればよい。あるいは、作成端末１０２が、組織に所属するドキュメント管理システムのユーザの情報を管理する後述のローカルユーザＩＤサーバ１５２（図１２参照）からユーザのリストを取得し、配信者が、組織内の他の処理装置１１０に登録されたユーザを配信先に選択できるようにしてもよい。この場合、配信先ユーザ選択メニュー４０

２では、各ユーザを、各々が登録された処理装置１１０が区別可能な表示形態で表示する。例えば、ユーザを、そのユーザが登録された処理装置１１０毎に異なる色や字体で表示してもよい。あるいはそのメニューを階層構造とし、まず処理装置１１０を選んでその処理装置１１０に登録されたユーザのリストを呼び出し、そのリストの中から配信先のユーザを選ぶ態様としてもよい。配信先ユーザリスト欄４０４には、ユーザが選んだ配信先ユーザのリストが表示される。配信者が配信先ユーザ選択メニュー４０２で配信先ユーザを選び、右側にある「追加」ボタンを押下すると、その配信先ユーザのユーザＩＤ又はユーザ名が配信先ユーザリスト欄４０４に追加される。また、配信者が配信先ユーザリスト欄４０４内の配信先ユーザを選び、右側の「削除」ボタンを押下すると、その配信先ユーザが配信先ユーザリスト欄４０４から削除される（すなわち配信先ではなくなる）。

【００９７】

配信先端末選択メニュー４０６は、そのドキュメントの配信先とする閲覧端末（ビューワ）１０４の選択肢を列挙するプルダウン形式のメニューである。選択肢となる閲覧端末１０４は処理装置１１０に登録されたものであり、選択肢となるそれら閲覧端末１０４のＩＤ及び端末名のリストは処理装置１１０から取得すればよい。あるいは、処理装置１１０自身やローカルユーザＩＤサーバ１５２（図１２参照。詳細は後述）等がドキュメント管理システムに登録された組織内の閲覧端末１０４のリストを有しており、作成端末１０２が、そのリストを配信者に提示して、組織内の他の処理装置１１０に登録されたユーザの閲覧端末１０４を配信先に選択できるようにしてもよい。配信先ユーザリスト欄４０４には、配信先ユーザリスト欄４０４の場合と同様、配信者が配信先端末選択メニュー４０６で選んだ配信先の閲覧端末１０４のリストが表示される。

【００９８】

なお、配信先のユーザ毎にそのユーザに対応する配信先の閲覧端末１０４を指定できるようにしてもよい。これには作成端末１０２は、例えば、配信先ユーザリスト欄４０４で配信先のユーザが選択される毎に、処理装置１１０（あるいはローカルユーザＩＤサーバ１５２又はユーザＩＤサーバ２１０）からそのユーザの既定の閲覧端末のリストを取得し、そのリストを配信先端末選択メニュー４０６に設定すればよい。配信者が配信先のユーザに対する配信先の閲覧端末１０４を明示的に選択しなかった場合は、そのユーザの既定の閲覧端末のリスト中の特定のもの（例えばリストの先頭）が自動的に配信先の閲覧端末１０４に選択される。

【００９９】

アクセス権限設定欄４１０は、そのドキュメントに対する配信先ユーザのアクセス権限（利用権限）を設定するための欄である。図示例では、閲覧、加工（編集）、印刷、コピーの４つの権限項目についてのチェックボックスが示されており、配信者は、そのドキュメントについて配信先ユーザに許可する項目のチェックボックスにチェックを入れる。

【０１００】

オフライン有効期間メニュー４１２は、ドキュメントに対して設定するオフライン有効期間の長さの選択肢を示すプルダウンメニューである。配信者は、オフライン有効期間メニュー４１２に示される数段階のオフライン有効期間の中から、今回システムに登録して配信するドキュメントに対して設定する期間を選ぶ。

【０１０１】

またオプション設定呼出ボタン４１４が押下されると、作成端末１０２は、図１０に例示するオプション設定画面４２０を表示する。オプション設定画面４２０は、処理装置指定欄４２２と元データ設定欄４２４を含む。処理装置指定欄４２２には、ドキュメントの送信先とする処理装置１１０の選択肢を示したプルダウンメニューが含まれる。このメニューには、作成端末１０２から選択可能な処理装置１１０のリストが含まれる。このリストに含まれる処理装置１１０は、まずその作成端末１０２が属するローカルシステム１００内にある処理装置１１０（基本は１つだが、複数あってもよい）である。また、同じ組織内の別のローカルシステム１００の処理装置１１０がそのリストに含まれていてもよい。元データ設定欄４２４には、ｅＤｏｃの元になった元データを処理装置１１０に保存す

るかの選択を受け付けるプルダウンメニューが表示される。
【０１０２】
ステップ（２）－１で作成端末１０２から処理装置１１０に送られる属性データには、このような設定画面により設定された、配信先情報（ユーザのリスト及び閲覧端末のリスト）、アクセス権限情報、オフライン有効期間、元データ情報等の情報が含まれる。
【０１０３】
図８の説明に戻る。
【０１０４】
（２）－２：　処理装置１１０は、作成端末１０２からドキュメント（対象ドキュメントと呼ぶ）及び属性データを受信する。
【０１０５】
（３）－１：　処理装置１１０は、ＤＩＤの発行権限及び発行枠を受け取っていない場合（あるいは受け取った発行枠を使い切った場合）は、管理システム２００のＤＩＤサーバ２２０に対して新たな発行権限及び発行枠を要求する。なお、受け取った発行枠に残りがある場合には、この要求を行わずに後述のステップ（４）に進む。
【０１０６】
（３）－２：　ＤＩＤサーバ２２０は、処理装置１１０からの要求に応じ、新たな発行権限及び発行枠をその処理装置１１０に送信する。
【０１０７】
（４）　処理装置１１０は、ＤＩＤサーバ２２０から付与された発行権限を用いてＤＩＤを発行し、そのＤＩＤを対象ドキュメントから生成するｅＤｏｃ（次のステップで生成する）に付与する。
【０１０８】
（５）－１：　処理装置１１０は、対象ドキュメントを暗号化するための暗号鍵を例えば乱数等を用いて生成する。また処理装置１１０は、対象ドキュメントをｅＤｏｃファイルへ変換する。すなわち、その対象ドキュメントをドキュメント管理システムの専用フォーマットへとエンコードし、エンコード結果を先ほど生成した暗号鍵で暗号化することでｅＤｏｃファイルを生成する。生成したｅＤｏｃファイルには先ほど生成したＤＩＤの情報を含める。
【０１０９】
（５）－２：　処理装置１１０は、生成したｅＤｏｃのメタデータを生成する。すなわち、作成端末１０２から受信した属性データに対して、先ほど生成したＤＩＤ、エンコードの日時、当該処理装置１１０のＩＤ、暗号化情報等を追加することでメタデータを生成する（図３参照）。ここで、暗号化情報には、配信先ユーザのそれぞれについて、暗号化に用いた暗号鍵をその配信先ユーザの公開鍵で暗号化した鍵情報が含まれる。
【０１１０】
（５）－３：　作成端末１０２から元データを保管する旨の指示を受け取った場合は、処理装置１１０は、作成端末１０２から受信したドキュメント（又はそのドキュメントの元になったアプリケーションデータ）を保存する。
【０１１１】
（６）－１：　処理装置１１０は、先ほど生成したＤＩＤをＤＩＤサーバ２２０にアップロードする。ＤＩＤサーバ２２０は、処理装置１１０からアップロードされたＤＩＤを保管する。
【０１１２】
（６）－２：　処理装置１１０は、先ほど生成したメタデータをメタデータサーバ２３０にアップロードする。メタデータサーバ２３０は、処理装置１１０からアップロードされてきたメタデータを保管する。
【０１１３】
（７）　処理装置１１０は、生成したｅＤｏｃの配信先の各閲覧端末１０４に対して、そのｅＤｏｃについての配信準備完了通知を送信する。この通知には、先ほど生成したＤ

ＩＤ、ｅＤｏｃのドキュメント名の情報を含む。また、この通知は、ｅＤｏｃの代表ページ（先頭ページ等の予め指定されたページ）のサムネイル画像を含んでいてもよい。

【０１１４】

さて、閲覧端末１０４を利用するユーザ（閲覧者と呼ぶ）は、自分の認証デバイス１３０を閲覧端末１０４のカードリーダ部に近づけることで、ユーザ認証を受ける。閲覧端末１０４は、自身に配信されているｅＤｏｃのリストを表示するリスト画面を表示する。図１１にこのリスト画面５００の例を示す。この例のリスト画面５００には、ｅＤｏｃ毎に、通知マーク５０２、そのｅＤｏｃのドキュメント名５０４、閲覧可否マーク５０６が含まれる。通知マーク５０２は、そのｅＤｏｃの状態を閲覧者に通知するためのマークである。通知マーク５０２が表すｅＤｏｃの状態には、「新着」（処理装置１１０からドキュメントが配信された後、まだ開かれていない状態。図では「☆」印で示す）、「正常」（図では無印）、「期限切れ」（アクセス有効期間が過ぎている状態。図では「！」印で示す）等がある。「期限切れ」状態については、閲覧端末１０４内にｅＤｏｃファイルが保存されていても、そのｅＤｏｃについての最新のメタデータを処理装置１１０又は管理システム２００から取得するまでは、閲覧できない。「正常」状態のｅＤｏｃについては、その閲覧端末１０４内には、アクセス有効期間が切れていないメタデータが保存（キャッシュ）されているので、仮に閲覧端末１０４が処理装置１１０や管理システム２００に対してオフライン状態となっていても閲覧可能である。閲覧可否マーク５０６は、閲覧端末１０４及びこれを使用しているユーザ（認証デバイス１３０により認証）の組合せが、当該閲覧端末１０４にキャッシュされたそのｅＤｏｃのメタデータに示されるそのｅＤｏｃの配信先のユーザ及び閲覧端末１０４の組合せに合致するか否かを示す。合致すればそのｅＤｏｃは閲覧可能（図では「○」印）、合致しなければ閲覧不可（図では「×」印）である。また、配信準備完了通知は受け取ったがまだｅＤｏｃファイル及びメタデータを受信していないｅＤｏｃについては、閲覧端末１０４は配信先の組合せに合致するか否かの判断基準の情報を持たないので、閲覧可否マーク５０６は、未定であることを示す「－」印となる。図示例では、上から３つのｅＤｏｃは、新着のものであり、まだｅＤｏｃ本体（ファイル及びメタデータ）の取得が済んでいないので、閲覧可否マーク５０６は未定を表すマークとなっている。

【０１１５】

閲覧者は、このリスト画面（図１１）上で、自分が閲覧したいｅＤｏｃを例えばタッチ操作等で選択し、閲覧指示を行う。ここでは、新着（通知マーク５０２が「☆」印）のｅＤｏｃが閲覧対象に選ばれたとする。

【０１１６】

（８）　図８の説明に戻る。閲覧端末１０４は、選ばれた閲覧対象のｅＤｏｃファイル及びメタデータを保持していないので、処理装置１１０から取得する必要がある。そこで、閲覧端末１０４は、自身が接続されているローカルネットワーク１０８上の処理装置１１０に対して、その閲覧者の認証デバイス１３０から取得した認証情報であるユーザＩＤキーを自身が接続されているローカルネットワーク１０８上に処理装置１１０に対して送信する。処理装置１１０は、そのユーザＩＤキーが自身に登録されているユーザを証明するものであるか検証する（ユーザ認証）。ここでは、そのユーザ認証が成功したとする。なお、閲覧端末１０４から受信したユーザＩＤキーが処理装置１１０に登録されたいずれのユーザにも該当しなかった場合、処理装置１１０は、そのユーザＩＤキーをユーザ認証に関する上位装置（ユーザＩＤサーバ２１０又はローカルユーザＩＤサーバ１５２）に送り、ユーザ認証を依頼してもよい。

【０１１７】

（９）－１：　また閲覧端末１０４は、処理装置１１０でのユーザ認証が成功したのを受けて、閲覧者が選択した閲覧対象のｅＤｏｃのＤＩＤを含む配信要求を処理装置１１０に送る。

【０１１８】

（９）－２：　処理装置１１０は、閲覧端末１０４からの配信要求に含まれるＤＩＤに

対応するｅＤｏｃファイル及びメタデータを、閲覧端末１０４に返信する。
【０１１９】
（１０） 閲覧端末１０４は、処理装置１１０から送られてきたｅＤｏｃファイル及びメタデータを受信して保存（キャッシュ）する。
【０１２０】
（１１） 閲覧端末１０４は、自身と、自身を現在使用中の閲覧者との組合せと一致する組合せが、そのメタデータ中の配信先情報（図３参照）に示される配信先ユーザと配信先端末の組合せの中にあるかどうかを判定する。ないと判定した場合は、閲覧者はその閲覧端末１０４ではそのｅＤｏｃファイルを閲覧できない。この場合、閲覧端末１０４は、閲覧できない旨を示すエラーメッセージを表示する。またこの場合、閲覧端末１０４は、保存しているそのｅＤｏｃファイル（及び対応するメタデータ）を削除してもよい。一方、閲覧端末１０４とそれを現在使用中の閲覧者との組合せに該当するものがメタデータ中の配信者情報内にあると判定した場合、閲覧端末１０４は、閲覧者に対してｅＤｏｃの閲覧を許可する。この場合、閲覧端末１０４は、そのメタデータ内の暗号化情報に含まれる各配信先ユーザに対応する暗号化済みの鍵の中から閲覧者に対応するものを取り出し、その鍵を閲覧者の秘密鍵（これは例えば認証デバイス１３０が保持している）で復号することで、ｅＤｏｃファイルの復号に必要な復号鍵を復元する。
【０１２１】
（１２） 閲覧端末１０４は、復元した復号鍵を用いてそのｅＤｏｃファイルを復号することで閲覧可能なドキュメントを再生し、そのドキュメントを出力（例えば画面表示）する。また、閲覧端末１０４は、閲覧者からそのドキュメントに対する操作指示を受け付けるかどうかを、メタデータに含まれるアクセス権限情報に従って制御する。閲覧端末１０４は、基本的には、復号したドキュメントをファイルに保存することはしない。すなわち、閲覧終了後は、閲覧端末１０４の不揮発性記憶装置には、ｅＤｏｃファイルとメタデータが保存されるが、復号結果のドキュメントは保存されない。
【０１２２】
次に、図１２を参照して、本実施形態のドキュメント管理システムの別の例を説明する。図１２に示す例では、企業等の組織のプライベートネットワークである組織内ネットワーク内にローカルシステム１００が複数存在する。そして、組織内ネットワークには、組織内管理システム１５０が設けられている。組織内管理システム１５０は、ドキュメント管理システムのうち当該組織内の処理やそれに必要な情報を管理する。すなわち、管理システム２００は、ドキュメント管理システムのサービスプロバイダが運用し、ドキュメント管理システムを利用する複数の組織についての情報や処理を管理するのに対し、組織内管理システム１５０はそれら情報や処理のうち当該組織に関する部分を、管理システム２００の管理下で管理する。
【０１２３】
組織内管理システム１５０は、ローカルユーザＩＤサーバ１５２、ローカルＤＩＤサーバ１５４、及びローカルメタデータサーバ１５６を有する。
【０１２４】
ローカルユーザＩＤサーバ１５２は、当該組織のメンバのうちドキュメント管理システムにユーザ登録されているユーザの情報を管理する。ローカルユーザＩＤサーバ１５２が保持する個々のユーザの情報は、図４に記載したユーザＩＤサーバ２１０が保持する一般ユーザの情報と同様である。処理装置１１０に対して、その処理装置１１０を取得し利用するユーザ（すなわちその処理装置１１０を「既定の処理装置」とするユーザ）が登録されると、処理装置１１０は登録されたユーザの情報を組織内のローカルユーザＩＤサーバ１５２に送る。ローカルユーザＩＤサーバ１５２は、受け取ったユーザの情報を保存すると共に、広域ネットワーク１０経由で中央の管理システム２００のユーザＩＤサーバ２１０に送る。ユーザＩＤサーバ２１０は、受け取ったユーザの情報を保管する。又、処理装置１１０に登録されたユーザの情報に変更が生じた場合、管理者等が処理装置１１０に対してそのユーザの情報の変更を行う。処理装置１１０は、このユーザ情報の変更内容の情

報（例えばユーザＩＤと、変更された情報項目の項目名と、その項目の変更後の値とを含む）をローカルユーザＩＤサーバ１５２に送信し、ローカルユーザＩＤサーバ１５２は、受信した変更に内容に応じて自身が保管している当該ユーザの情報を変更する。また、ローカルユーザＩＤサーバ１５２は、受け取った変更内容の情報を中央のユーザＩＤサーバ２１０に送り、ユーザＩＤサーバ２１０は送られてきた情報に応じて、自分が保持するそのユーザの情報を変更する。

【０１２５】

ローカルＤＩＤサーバ１５４は、当該組織の組織内ネットワークに属する各ローカルシステム１００内の処理装置１１０が発行したＤＩＤを受け取り、保管する。ローカルＤＩＤサーバ１５４が保持する情報は、図５に記載したＤＩＤサーバ２２０が保持する情報と同様である。またローカルＤＩＤサーバ１５４は、処理装置１１０から受け取ったＤＩＤの情報を中央のＤＩＤサーバ２２０に送り、ＤＩＤサーバ２２０はその情報を保管する。また、ローカルＤＩＤサーバ１５４は、中央のＤＩＤサーバ２２０からＤＩＤの発行権限及び発行枠を付与され、その発行枠の範囲内で、その発行権限に基づいて管理下の各処理装置１１０に対してＤＩＤの発行権限及び発行枠を付与する。

【０１２６】

ローカルメタデータサーバ１５６は、当該組織の組織内ネットワークに属する各ローカルシステム１００内の処理装置１１０が生成したｅＤｏｃのメタデータを受け取り、保管する。ローカルメタデータサーバ１５６が保持する情報は、メタデータサーバ２３０が保持する情報と同様である。またローカルメタデータサーバ１５６は、処理装置１１０から受け取ったメタデータを中央のメタデータサーバ２３０に送り、メタデータサーバ２３０はそのメタデータを保管する。

【０１２７】

図１２のシステムでは、処理装置１１０は、自分には登録されていないが同じ組織内の他の処理装置１１０に登録されているユーザからのドキュメントの登録（及び配信）要求、又はｅＤｏｃファイル又はメタデータの取得要求等の要求を受けた場合、組織内管理システム１５０を介してそれら要求に応答する。

【０１２８】

１つの例として、組織内ネットワーク内の第１の部署にある第１のローカルシステム１００内の処理装置＃１に登録されている閲覧者が、その処理装置＃１に登録され配信されたｅＤｏｃを自分の閲覧端末１０４に保存し、その後処理装置＃２の管理下にある第２の部署に移動してそのｅＤｏｃを閲覧しようとしたときのことを考える。この時点では、その閲覧端末１０４内に保存されたそのｅＤｏｃのメタデータは古くなっている（すなわちアクセス有効期間が過ぎている）ものとする。この場合、閲覧者がその閲覧端末１０４でそのｅＤｏｃを開く操作を行った場合、図１３に示す処理が行われる。

【０１２９】

まず、閲覧端末１０４は、自身が今接続している第２のローカルシステム１００のローカルネットワーク１０８から処理装置１１０を探す。これにより処理装置＃２が見つかる。この処理装置＃２は、そのｅＤｏｃを配信した処理装置＃１とは別の装置なので、そのｅＤｏｃファイルやメタデータは持っていない。

【０１３０】

（１）　閲覧端末１０４は、閲覧者の認証デバイス１３０からユーザＩＤキー（認証情報）を読み込む。

【０１３１】

（２）　閲覧端末１０４は、閲覧の対象として指示されたそのｅＤｏｃの最新のメタデータを取得するためのユーザ認証のために、その処理装置＃２に対して、認証デバイス１３０から取得したユーザＩＤキーを送信する。

【０１３２】

（３）　閲覧端末１０４は、そのｅＤｏｃのメタデータを処理装置＃２に要求する。この要求には、そのｅＤｏｃのＤＩＤが含まれる。

【０１３３】
（４）－１： 処理装置＃２は、閲覧端末１０４から受け取ったユーザＩＤキーが自身に登録されたユーザのものかどうかを調べる（ユーザ認証）。この例では、その閲覧者は処理装置＃１に登録されており、処理装置＃２には登録されていないので、処理装置＃２は、予め設定されているローカルユーザＩＤサーバ１５２のアドレスに対して、そのユーザＩＤキーを含む認証要求を送る。また、処理装置＃２は、閲覧端末１０４からのメタデータ要求に含まれるＤＩＤを、予め設定されているローカルＤＩＤサーバ１５４に送り、認証を求める。
【０１３４】
（４）－２： ローカルユーザＩＤサーバ１５２は、処理装置＃２から受け取ったユーザＩＤキーが、自身に登録されているユーザのものであるかどうかを検証する（ユーザ認証）。そのユーザＩＤキーの持ち主である閲覧者は、処理装置＃１に登録されているので、その上位装置であるローカルユーザＩＤサーバ１５２にもユーザ登録がなされている。したがって、このユーザ認証は成功する。ローカルユーザＩＤサーバ１５２は、認証が成功したことを示す応答を処理装置＃２に返す。
【０１３５】
またローカルＤＩＤサーバ１５４は、閲覧端末１０４から送られてきた検証対象のＤＩＤが正当なＤＩＤであるかどうか、すなわち自身が保存しているＤＩＤであるかどうかを調べる。この例では、そのｅＤｏｃのＤＩＤは、処理装置＃１が発行したものであり、処理装置＃１のＤＩＤに関する上位装置であるローカルＤＩＤサーバ１５４にも保存されている。したがって、そのＤＩＤは正当なものであると認証される。ローカルＤＩＤサーバ１５４は、ＤＩＤが正当であると認証する旨の応答を処理装置＃２に返す。
【０１３６】
（５）－１： ユーザ認証及びＤＩＤ認証が成功したので、処理装置＃２は、閲覧端末１０４からのメタデータ要求に応えるための処理を続行する。すなわち、処理装置＃２は、ＤＩＤを含むメタデータ要求を、あらかじめ設定されているローカルメタデータサーバ１５６のアドレスに送る。
【０１３７】
（５）－２： ローカルメタデータサーバ１５６は、処理装置＃２からメタデータ要求を受けると、その要求に含まれるＤＩＤに対応するメタデータを処理装置＃２に返す。ｅＤｏｃのメタデータは、配信者から処理装置１１０にて変更されると、その変更が即座にローカルメタデータサーバ１５６に反映されるので、このとき処理装置＃２に返されるメタデータは、閲覧対象のｅＤｏｃのメタデータの最新版である。
【０１３８】
（６） 処理装置＃２は、ローカルメタデータサーバ１５６から受け取ったメタデータを、閲覧端末１０４に対して送信する。
【０１３９】
（７） 閲覧端末１０４は、処理装置＃２からメタデータを受信し、保存（キャッシュ）する。
【０１４０】
（８） 閲覧端末１０４は、受け取った最新のメタデータの配信先情報を参照し、閲覧端末１０４及び閲覧者の組合せの権限チェックを行う。すなわち、閲覧端末１０４自身と閲覧者との組合せと一致する組合せが、その配信先情報（図３参照）に示される配信先ユーザと配信先端末の組合せの中にあれば、閲覧権限ありと判定し、なければ閲覧権限なしと判定する。閲覧権限なしと判定した場合、閲覧端末１０４はエラー表示を行う。閲覧権限ありと判定した場合、閲覧端末１０４は、そのメタデータ内の暗号化情報に含まれる各配信先ユーザに対応する暗号化済みの鍵の中から閲覧者に対応するものを取り出し、その鍵を閲覧者の秘密鍵（これは例えば認証デバイス１３０が保持している）で復号することで、ｅＤｏｃファイルの復号に必要な復号鍵を復元する。
【０１４１】

（９）　そして閲覧端末１０４は、復元した復号鍵を用いてそのｅＤｏｃファイルを復号することで閲覧可能なドキュメントを再生し、そのドキュメントを出力（例えば画面表示）する。そして、閲覧者からそのドキュメントに対する操作指示を受け付けるかどうかを、メタデータに含まれるアクセス権限情報に従って制御する。

【０１４２】

次に、図１４を参照して、第１のローカルシステム１００内の処理装置＃１に登録されているユーザが、処理装置＃２の管理下にある第２の部署でドキュメントをドキュメント管理システムに登録する場合の処理の流れを考える。そのユーザ（ドキュメントの配信者）は、処理装置＃２には登録されていないとする。

【０１４３】

（１）　ユーザは、自分の作成端末１０２にドキュメントの登録を指示すると、作成端末１０２はログイン認証情報の入力を求める画面を表示する。配信者がその求めに応じて認証情報（例えばユーザＩＤ及びパスワード）を入力すると、作成端末１０２は、その認証情報をローカルネットワーク１０８経由で処理装置１１０に送信する。

【０１４４】

（２）　処理装置＃２は、作成端末１０２から受け取った認証情報が自身に登録されたユーザのものであるか判定する。この場合、配信者は処理装置＃２に登録されていない。この場合、処理装置＃２は、上位のローカルユーザＩＤサーバ１５２に対してその認証情報を送り、認証を求める。

【０１４５】

（３）　ローカルユーザＩＤサーバ１５２は、受け取った認証情報が自身に登録されているユーザのものかどうか判定する（ユーザ認証）。この例では、配信者は処理装置＃１に登録されているユーザなので、ローカルユーザＩＤサーバ１５２にも登録されており、このユーザ認証は成功する。ローカルユーザＩＤサーバ１５２は、処理装置＃２に対して、ユーザ認証が成功したことを示す情報を返す。

【０１４６】

（４）　処理装置＃２は、ローカルユーザＩＤサーバ１５２から認証成功の旨の応答を受けると、作成端末１０２に対してユーザ認証が成功した旨を応答する。

【０１４７】

（５）　作成端末１０２は、ユーザ認証が成功した場合、ユーザが登録対象に選択したドキュメントと、ユーザが入力した属性データとを処理装置＃２に送る。

【０１４８】

（６）　処理装置＃２は、作成端末１０２からドキュメント及び属性データを受信する。

【０１４９】

（７）－１：　処理装置＃２は、ＤＩＤの発行権限及び発行枠を使い切った場合は、ローカルＤＩＤサーバ１５４に対して新たな発行権限及び発行枠を要求する。なお、受け取った発行枠に残りがある場合には、この要求を行わずに後述のステップ（８）に進む。

【０１５０】

（７）－２：　ローカルＤＩＤサーバ１５４は、処理装置＃２からの要求に応じ、新たな発行権限及び発行枠をその処理装置＃２に付与する。なお、中央のＤＩＤサーバ２２０から付与された発行枠を使い切った場合、ローカルＤＩＤサーバ１５４は、ＤＩＤサーバ２２０に新たな発行権限及び発行枠を要求し、これに応じて付与された発行権限及び発行枠を用いて、処理装置＃２にＤＩＤの発行権及び発行枠を付与する。

【０１５１】

（８）　処理装置＃２は、付与された発行権限を用いてＤＩＤを発行し、そのＤＩＤを対象ドキュメントから生成するｅＤｏｃ（次のステップで生成する）に付与する。

【０１５２】

（９）－１：　処理装置＃２は、対象ドキュメントを暗号化するための暗号鍵を生成し、対象ドキュメントを本システムの専用フォーマットへとエンコードし、エンコード結果

を先ほど生成した暗号鍵で暗号化することでｅＤｏｃファイルを生成する。
【０１５３】
（９）－２： 処理装置＃２は、作成端末１０２から受信した属性データに対して、先ほど生成したＤＩＤ、エンコードの日時等の項目を追加することで、ｅＤｏｃのメタデータを生成する。
【０１５４】
（１０） 処理装置＃２は、生成したＤＩＤをローカルＤＩＤサーバ１５４に、生成したメタデータをローカルメタデータサーバ１５６に、それぞれアップロードする。ローカルＤＩＤサーバ１５４は、処理装置＃２からアップロードされたＤＩＤを、その中に含まれる発行権限キーに対応する発行済ＤＩＤリスト（図５参照）に追加すると共に、中央のＤＩＤサーバ２２０にアップロードする。ＤＩＤサーバ２２０は、ローカルＤＩＤサーバ１５４からアップロードされたＤＩＤを、発行権限キーに対応する発行済ＤＩＤリスト（図５参照）に追加する。またローカルメタデータサーバ１５６は、処理装置＃２からアップロードされたメタデータを保管すると共に、中央のメタデータサーバ２３０にアップロードする。メタデータサーバ２３０は、ローカルメタデータサーバ１５６からアップロードされたメタデータを保管する。
【０１５５】
処理装置＃２は、生成したｅＤｏｃを配信者の指定した配信先に配信する。この処理は、図８のステップ（７）乃至（１２）と同様である。
【０１５６】
（１１） また処理装置＃２は、生成したｅＤｏｃファイル及びメタデータを作成端末１０２に送信する。処理装置＃２は、そのｅＤｏｃファイル及びメタデータを保存してもよいし、保存せずに削除してもよい。保存せずに削除する場合、それらｅＤｏｃファイル及びメタデータは、組織内の処理装置１１０群のうち、後述するステップ（１３）により既定の処理装置である処理装置＃１のみに保存されることになる。配信者の既定の処理装置でない処理装置１１０がその配信者から登録・配信依頼されたｅＤｏｃファイル及びメタデータを保存するか否かは、処理装置１１０に設定可能としてもよい。
【０１５７】
（１２） 作成端末１０２は、処理装置１１０から受け取ったｅＤｏｃファイル及びメタデータを、後でその配信者の既定の処理装置である処理装置＃１に転送するために保存する。
【０１５８】
（１３） 配信者は、作成端末１０２を持って自分の所属する第１の部署に戻った際、作成端末１０２は、第１のローカルネットワーク１０８上でその配信者の既定の処理装置である処理装置＃１を探す。処理装置＃１を見つけると、作成端末１０２は、上記ステップ（１２）で保存していたｅＤｏｃファイル及びメタデータを処理装置＃１に登録する。これにより、配信者は、メタデータの内容（例えば配信先）を変更したい場合には、既定の処理装置＃１にアクセスしてその変更の操作を行えばよい。
【０１５９】
以上に説明した本実施形態のドキュメント管理システムでは、作成端末１０２から処理装置１１０に配信を指示したドキュメントの本体情報（すなわちｅＤｏｃファイル）は、処理装置１１０と配信先の閲覧端末１０４が持つのみで、その他のネットワークや装置には出回らない。このためｅＤｏｃファイルの漏洩リスクが極小化される。特にｅＤｏｃファイルの配信先を、そのｅＤｏｃを生成したローカルネットワーク１０８上の閲覧端末１０４に限定すれば、ｅＤｏｃはそのローカルネットワーク１０８から外に一切出ないことになる。
【０１６０】
一方、ｅＤｏｃのメタデータは、中央の管理システム２００や組織毎の組織内管理システム１５０に登録されており、閲覧端末１０４がいろいろな場所に移動しても、広域ネットワーク１０や組織のプライベートネットワークを介して入手可能となっている。閲覧端

末１０４は、ｅＤｏｃの閲覧指示をユーザから受けた場合、そのｅＤｏｃの最新のメタデータを組織内管理システム１５０又は中央の管理システム２００から取得し、その最新のメタデータに含まれる配信先情報に基づき、そのユーザにそのｅＤｏｃの閲覧を許可してよいかどうかを判定する。そのユーザが、そのｅＤｏｃの登録・配信時には配信先に指定されていても、その後の配信先変更で配信先から外れている場合には、閲覧は許可されない。

【０１６１】

図１３及び図１４の例では、処理装置＃１及び処理装置＃２は共に同じ組織内に設置されたものであり、配信先のユーザもその組織に所属していると想定しているので、ユーザ認証はその組織のローカルユーザＩＤサーバ１５２で行った。これに対し、閲覧者が処理装置＃２とは異なる組織に属するユーザの場合、処理装置＃２でもその上位のローカルユーザＩＤサーバ１５２でもその配信者を認証できない。この場合、更に上位のユーザＩＤサーバ２１０がその配信者のユーザ認証を行ってもよい。

【０１６２】

図１３及び図１４の例では、別の処理装置＃２が、処理装置＃１に登録されたユーザの閲覧端末１０４と、ローカルユーザＩＤサーバ１５２やローカルメタデータサーバ１５６とのやりとりの仲立ちをした。しかし、これは一例に過ぎない。この代わりに、例えば、処理装置＃２は、閲覧端末１０４から送られてきたユーザの認証情報からそのユーザが処理装置＃２に登録されたものでない場合、閲覧端末１０４に対して認証不可の応答を行えばよい。この場合、閲覧端末１０４は、自機に登録されている上位装置のアドレス情報を用いて、ローカルユーザＩＤサーバ１５２に認証を求め、認証が成功すると、ローカルメタデータサーバ１５６にアクセスして必要なメタデータを取得する。

【０１６３】

図１３の例は、ユーザは自分の所属する組織内の、自分の既定の処理装置とは別の処理装置１１０の管理下にあるローカルシステム１００に移動してドキュメントの閲覧を行う場合の例であった。しかしながら、ユーザが、自分の所属する組織の外で、自分の既定の処理装置から配信されたドキュメントを閲覧できるようにしてもよい。この場合、ユーザの閲覧端末１０４は、中央の管理システム２００内のユーザＩＤサーバ２１０で認証を受け、閲覧したいドキュメントのメタデータをメタデータサーバ２３０から取得する。

【０１６４】

＜ＤＩＤの例＞

次に、図１５を参照して、ドキュメント管理システムでｅＤｏｃの識別情報に用いるＤＩＤ６００の構成について説明する。

【０１６５】

図示のようにＤＩＤ６００は、発行権限キー６０２、処理装置固有情報６０４、発行年月日６０６、発行証明キー６０８、及び発行番号６１０を含む。なお、図示のＤＩＤ６００及びその構成要素６０２～６１０の桁数はあくまで例示的なものにすぎない。

【０１６６】

発行権限キー６０２は、ＤＩＤサーバ２２０が処理装置１１０に付与した発行権限を識別するキー情報である。ＤＩＤサーバ２２０は、処理装置１１０から発行権限及び発行枠の要求を受けた場合、発行権限キー６０２を生成し、その発行権限キー６０２を発行枠（例えばドキュメント数１００個）の数値と共に処理装置１１０に送信する。なお、ＤＩＤサーバ２２０と処理装置１１０との間にローカルＤＩＤサーバ１５４が介在するシステム構成の場合には、ＤＩＤサーバ２２０がローカルＤＩＤサーバ１５４に対して、例えば、発行権限キーと発行枠の組を複数組一括して付与する。この付与は、ＤＩＤサーバ２２０が、それら複数組の発行権限キー及び発行枠を処理装置１１０に付与する処理をローカルＤＩＤサーバ１５４に依頼することと捉えてもよい。ローカルＤＩＤサーバ１５４は、管理下の処理装置１１０から発行権限を要求された場合、付与された複数組の発行権限キー及び発行枠の中の未付与のものをその処理装置１１０に付与すればよい。

【０１６７】

処理装置固有情報６０４は、そのＤＩＤを発行した処理装置１１０に固有な情報である。すなわち、ＤＩＤ６００中の処理装置固有情報６０４を調べることで、そのＤＩＤ６００を発行した処理装置１１０が一意に特定できる。処理装置固有情報６０４は、処理装置１１０が保持している。

【０１６８】

発行年月日６０６は、そのＤＩＤを発行した年月日を示す文字列である。ＤＩＤの発行年月日は、そのＤＩＤの付与先であるｅＤｏｃを生成（エンコード）した年月日でもある。

【０１６９】

発行証明キー６０８は、その処理装置１１０（処理装置固有情報６０４により特定される）が、発行権限キー６０２が示す発行権限を用いてそのＤＩＤを発行したことを証明するキー情報である。発行証明キー６０８は、例えば、発行権限キー６０２をその処理装置１１０の秘密鍵で暗号化することで得られる値である。この場合、発行証明キー６０８をその処理装置１１０の公開鍵で復号して得られた値が、発行権限キー６０２に一致すれば、そのＤＩＤ６００は、その発行権限キー６０２を用いてその処理装置１１０が発行したものであることが証明される。また、ＤＩＤ６００のうち発行権限キー６０２を除く部分の値（又はその値から生成した所定桁数のハッシュ値）を処理装置１１０の秘密鍵で暗号化して得た値を発行証明キー６０８としてもよい。この場合、発行証明キー６０８を処理装置１１０の公開鍵で復号した値が、ＤＩＤ６００の発行証明キー６０８を除いた部分の値と矛盾しなければ（例えば復号結果がその値のハッシュ値と一致）、そのＤＩＤ６００は発行権限キー６０２に基づきその処理装置１１０が発行したものであり、ＤＩＤ６００の発行証明キー６０８以外の部分に改ざんがないことが証明される。

【０１７０】

発行番号６１０は、そのＤＩＤ６００が、処理装置１１０がその発行権限キー６０２を用いて発行した何番目のＤＩＤであるかを示す通し番号である。ある発行権限キー６０２を用いて生成されたＤＩＤ６００の発行番号６１０が取り得る最大値は、その発行権限キー６０２と共にＤＩＤサーバ２２０（又はローカルＤＩＤサーバ１５４）が付与した発行枠の値（ドキュメント数）である。

【０１７１】

＜登録後の配信先変更＞

さて、ｅＤｏｃをドキュメント管理システムに登録した後、配信者（あるいは配信先の変更権限を与えられた他の者）が、配信先の削除や追加、それら配信先に与えたｅＤｏｃへのアクセス権限を修正したくなることも考えられる。そのような場合、配信者は、作成端末１０２又は閲覧端末１０４（以下ユーザ端末と総称）を用いて例えば既定の処理装置１１０にアクセスし、対象となるｅＤｏｃのＤＩＤを指定して、配信先（又はアクセス権限）の編集処理の実行を指示する。

【０１７２】

この指示を受けた処理装置１１０は、ユーザ認証によりその指示を発したユーザがその対象ｅＤｏｃの正しい配信者等（配信者及び配信先変更権限を与えられた他の者の総称）であることを確認した場合、配信先及びアクセス権限の編集画面をユーザ端末に提供する。編集画面は、図９に示した入力画面４００と同様のものでよい。配信者等は、その編集画面上で、配信先のユーザ及び閲覧端末の追加や削除、アクセス権限内容の変更を行う。配信者等が、編集画面上で必要な変更を行った後、その変更を確定する操作を行うと、処理装置１１０は、保存しているそのｅＤｏｃのメタデータにその変更を反映させると共に、その変更内容を上位のローカルメタデータサーバ１５６及びメタデータサーバ２３０に通知する。ローカルメタデータサーバ１５６及びメタデータサーバ２３０は、通知された変更内容を、保存しているそのｅＤｏｃのメタデータに反映させる。例えば、配信時には配信先に指定されていたユーザであっても、その後の変更で配信先から削除された場合、そのｅＤｏｃの閲覧が不可となる。また、処理装置１１０は、このようにｅＤｏｃのメタデータ中の配信先情報が変更された場合、変更前の配信先情報には含まれていたが、変更

後の配信先情報には含まれていない配信先の閲覧端末１０４に対して、そのｅＤｏｃファイル（及び対応するメタデータ）を削除する指示を送ってもよい。

【０１７３】

以上の例では、処理装置１１０がｅＤｏｃの配信先やアクセス権限の変更指示を受け付けたが、この代わりに又はこれに加えて、上位装置、すなわち管理システム２００（メタデータサーバ２３０）又は組織内管理システム１５０（ローカルメタデータサーバ１５６）がその変更指示を受けてもよい。この場合、上位装置は、そのｅＤｏｃを生成した処理装置１１０（及びその処理装置１１０が属する組織のローカルメタデータサーバ１５６）に対して、その変更指示に応じて変更された新たなメタデータを送信し、処理装置１１０内の既存のメタデータと置き換えさせるようにする。

【０１７４】

＜処理装置のステータス管理＞

次に、処理装置１１０のステータス管理に基づく制御について説明する。

【０１７５】

処理装置１１０は、定期的に自身のステータスを管理システム２００に通知する。管理システム２００では、処理装置管理サーバ２４０が、受け取ったステータスを、その受け取りの日時と対応付けて当該処理装置１１０についてのステータス履歴２４２に追加する。また処理装置管理サーバ２４０は、受け取ったステータスについてチェックを行い、そのチェックの結果に従って、処理装置１１０のユーザに対するサービス提供の可・不可を制御する。

【０１７６】

処理装置１１０が処理装置管理サーバ２４０に定期送信するステータスは、図６に例示した処理装置のステータス２４４と同様の項目を含む（ただし、ステータス２４４のうち処理装置１１０によっては変更されることがない設置場所やエンコード回路情報、処理装置の製造者名等は定期送信しなくてよい）。

【０１７７】

処理装置管理サーバ２４０は、処理装置１１０から送られてくるステータスに基づき、例えば図１６に例示する処理を実行する。

【０１７８】

まず、処理装置管理サーバ２４０は、処理装置１１０からステータスを受信すると（Ｓ１００）、そのステータスのうちの検査対象項目の値を、それぞれの項目の基準と照合する（Ｓ１０２）。検査対象項目には、暗号化ソフトの名称及びバージョン、エンコードソフトの名称及びバージョン、処理装置１１０にインストールされているセキュリティ証明書、処理装置１１０にインストールされている暗号鍵（例えば秘密鍵と公開鍵ペア。通信路暗号化や署名的な目的等に用いる）の情報（例えば当該鍵の識別情報やインストール日時等）、エンコード回路の名称及びファームウエア（ＦＷ）のバージョン、搭載フォント種類、ディスク（二次記憶）の空き容量、が含まれる。また、個々の項目についての基準の例としては、暗号化ソフトやエンコードソフト、ファームウエアが最新バージョンであること（あるいはあるバージョン以降のバージョンであること）、ディスクの空き容量が所定の閾値以上であること、インストールされているセキュリティ証明書の中にブラックリストに入っている証明書がないこと、処理装置１１０の暗号鍵がインストールされた日から所定期間が経過していないこと、所定（すなわちあらかじめ定めた）種類のフォントがインストールされていること、などがある。

【０１７９】

例えば、処理装置１１０が通信路暗号化や署名等に用いる暗号鍵は、その安全性を維持するために、定期的に新しい鍵に変更することが望ましいので、インストール日時から所定期間が経過した以降は基準を満たさないものと判定してサービス提供を不可とし（あるいは不可となる旨の警告を発し）、新しい鍵への交換を促す。

【０１８０】

次に処理装置管理サーバ２４０は、処理装置１１０から受け取ったステータスの検査対

象項目の中に、当該項目の基準を満たさないものがあるかどうかを判定し（Ｓ１０４）、なければ今回ステータスを受信した処理装置１１０についての処理を終了する。Ｓ１０４で基準を満たさない項目があった場合、処理装置管理サーバ２４０は、その処理装置１１０に対してサービス不可を通知する（Ｓ１０６）。この通知を受けた処理装置１１０は、本実施形態のドキュメント管理システムに対するドキュメントの登録（配信）サービスを停止する。すなわち、作成端末１０２からのドキュメントの登録（配信）要求を受け付けず、サービス停止中である旨のメッセージを返す。

【０１８１】

このような制御によれば、処理装置１１０が基準を満たさない品質のｅＤｏｃを生成してしまう可能性が低減される。例えば、この制御によれば、古い暗号化ソフトにより暗号化の強度が十分でないｅＤｏｃが生成される前に、その処理装置１１０のサービスが停止される。また、ディスク空き容量が少なかったりファームウエアが古かったりしてｅＤｏｃの生成処理にエラーが生じ、それが元でドキュメントの漏洩が生じるといった事態が起こる前に、サービスが停止される。また、所定のフォントを持たない処理装置１１０がドキュメント中のそのフォントを別のフォントに置き換えてエンコードしてしまうことによるｅＤｏｃの画質低下が起こる前に、サービスが停止される。エンコード回路のファームウエアが古いため、最新のファームウエアがサポートしているドキュメントの画像サイズがサポートされておらず、ｅＤｏｃの画像サイズが制限されてしまう等の事態も生じにくくなる。

【０１８２】

なお、ステータスの検査対象項目に、ｅＤｏｃのセキュリティに影響する項目とそうでない項目の分類を設け、処理装置１１０にサービスを停止させるのは、前者の項目が基準を満たさない場合に限ってもよい。後者の項目が基準を満たさない場合は、処理装置１１０やその管理者に警告を送り、その項目についての不具合を解消するよう促す。この警告を受けて、処理装置１１０の管理者は、自分で対処できる項目については処理装置１１０の修理を行い、専門の保守作業員の介入が必要な項目については、保守作業員の派遣をシステム運営者に依頼する。また、検査対象項目のうちの特定項目が基準を満たさないことが分かった場合に、処理装置管理サーバ２４０が、当該処理装置１１０に対して保守作業員を派遣する手配を自動的に行ってもよい。

【０１８３】

図１６の処理の変形例を、図１７を参照して説明する。

【０１８４】

図１７の手順では、処理装置１１０のステータスの検査対象項目に、緊急項目とそれ以外というレベル分けを導入している。緊急項目は、処理装置１１０が生成するｅＤｏｃのセキュリティ上の品質やドキュメント管理システムのセキュリティに大きな影響を与える項目である。その項目が基準を満たさない処理装置１１０が生成したｅＤｏｃは十分な安全性が確保されないか、またはその項目が基準を満たさない処理装置１１０が稼働を続けると、その処理装置１１０がドキュメント管理システムのセキュリティホール（脆弱性）となってしまう可能性がある。そのような緊急項目の対象の例としては、暗号化ソフトのバージョン、処理装置１１０にインストールされているセキュリティ証明書、処理装置１１０にインストールされている暗号鍵に脆弱性が見つかった場合等がある。

【０１８５】

緊急項目が基準を満たさないことによる問題を避ける１つの方法は、緊急項目が基準を満たさない処理装置１１０を停止させ、保守作業員を派遣してその緊急項目についての修正・修理を行わせることである。しかし、修正が完了するまでの間、ユーザはその処理装置１１０を使えないという不便がある。

【０１８６】

そこで、図１７の手順では、処理装置管理サーバ２４０は、Ｓ１０４で基準を満たさない項目を見つけた場合、その項目が緊急項目であるかどうかを判定する（Ｓ１１０）。そして、緊急項目である場合、その緊急項目の不具合を修正するための設定情報を処理装置

管理サーバ２４０からその処理装置１１０に対して、広域ネットワーク１０を経由してリモートインストールする（Ｓ１１２）。緊急項目の不具合を修正するための設定情報の例としては、最新バージョンの暗号化ソフト、脆弱性が見つかったセキュリティ証明書に対する脆弱性が解消された最新版のセキュリティ証明書、処理装置１１０の脆弱性が見つかった秘密鍵・公開鍵のペアを置き換える新たな鍵ペア、等がある。

【０１８７】

例えば新たな鍵ペアの場合、その新たな鍵ペアを生成するためのフレーズを処理装置管理サーバ２４０が用意してそのフレーズを用いて鍵ペアを生成し、生成した鍵ペアをセキュアな方法で処理装置１１０に伝送してリモートインストールする。

【０１８８】

これにより処理装置１１０内の基準を満たさない緊急項目についての設定情報が基準を満たすものへと更新される。またこの更新に応じて、その処理装置１１０が持つステータスのうちのその緊急項目の値が更新される。

【０１８９】

またＳ１１０の判定結果がＮｏ（緊急項目に該当しない）の場合、処理装置管理サーバ２４０は、処理装置１１０又は管理者に対して基準を満たさない項目を示す警告を送り、その処理装置１１０のその項目についての修正のために保守作業員の派遣の手配を行う（Ｓ１１４）。緊急項目でない項目については、処理装置１１０がそのまま稼働を続けてもセキュリティ上の重大な問題は生じにくいので、処理装置１１０は停止させず、保守作業員の派遣により対処するのである。緊急項目以外の項目については、処理装置管理サーバ２４０がリモートインストールしなくてよいので、処理装置管理サーバ２４０の負荷増大が避けられる。

【０１９０】

図１７の例では、緊急項目についての設定情報を処理装置管理サーバ２４０からトップダウンで処理装置１１０にインストールし、これに応じて処理装置１１０にてその設定情報がインストールされ、処理装置１１０のステータスのうちその緊急項目の値が更新される。これに対して、緊急項目以外のステータスの項目については、個々の処理装置１１０にて、例えば保守作業員により値の設定や変更を行い、その項目に対応する設定情報（例えば暗号化ソフトの最新バージョン）のインストールを行う。このように処理装置１１０で行われたステータス項目値の設定や変更は、上位の処理装置管理サーバ２４０に通知され、処理装置管理サーバ２４０は、その通知に応じて自身が持つその処理装置１１０のステータスの対応項目の値を変更する。

【０１９１】

＜ＤＩＤの検証＞

管理システム２００は、処理装置１１０が発行したＤＩＤを通知してきた際や、閲覧端末１０４からメタデータの要求（この要求はＤＩＤを含む）を送ってきた際、あるいはＤＩＤの検証の依頼をユーザ等から受けた際に、そのＤＩＤが正しいものかどうかを検証する。

【０１９２】

この場合ＤＩＤサーバ２２０は、対象のＤＩＤ６００（図１５参照）について以下の点を検証する。

【０１９３】

（ａ）ＤＩＤ６００中の発行権限キー６０２と処理装置固有情報６０４との間に矛盾がないこと。

【０１９４】

ＤＩＤサーバ２２０は、その発行権限キー６０２が、自身の記録している情報（図５参照）の中に、その処理装置固有情報６０４が示す処理装置１１０を付与先とする発行権限キーとして記録されているかどうか調べる。記録されていなければ、その発行権限キー６０２はその処理装置固有情報６０４が示す処理装置１１０に発行されたことがないものなので、それら両者は矛盾する。この場合、そのＤＩＤ６００は不正なＤＩＤである。

【０１９５】
（ｂ）ＤＩＤ６００中の発行権限キー６０２と発行年月日６０６とが矛盾しないこと。
【０１９６】
ＤＩＤサーバ２２０は、発行権限キーに対応づけて、キー付与日時とキー終了日時を記録している（図５参照）。ＤＩＤ６００中の発行年月日６０６が、ＤＩＤ６００中の発行権限キー６０２に対応付けて記録されているキー付与日時からキー終了日時までの期間から外れている場合、発行権限キー６０２と発行年月日６０６は矛盾している。この場合、ＤＩＤ６００は不正なＤＩＤである。
【０１９７】
（ｃ）ＤＩＤ６００中の発行権限キー６０２、処理装置固有情報６０４及び発行証明キー６０８の間に矛盾がないこと。
【０１９８】
ＤＩＤサーバ２２０は、発行証明キー６０８を、その処理装置固有情報６０４が示す処理装置１１０の公開鍵で復号し、その復号結果が示す発行証明キーが、ＤＩＤ６００中のその発行証明キー６０８と一致するかどうかを判定する。一致しない場合、それら三者の間には矛盾が存在し、ＤＩＤ６００は不正なものであると分かる。
【０１９９】
（ｄ）ＤＩＤ６００中の発行番号６１０が、発行権限キー６０２に対応する発行枠と矛盾しないこと。
【０２００】
ＤＩＤサーバ２２０は、発行権限キー６０２と共に処理装置１１０に付与した発行枠を記録している（図５参照）。ＤＩＤ６００中の発行番号６１０が、発行権限キー６０２に対応して記録されている発行枠よりも大きい番号である場合、そのＤＩＤは不正なものである。
【０２０１】
（ｅ）ＤＩＤ６００中の発行番号６１０が、そのＤＩＤ６００の発行権限キー６０２と同じ発行権限キーを含む発行済みのＤＩＤの発行番号と矛盾しないこと。この基準は、処理装置１１０から新たに発行したＤＩＤを通知された場合に、そのＤＩＤが既に発行済みのものと矛盾するかどうかの検証に用いる。
【０２０２】
ＤＩＤサーバ２２０は、発行権限キーに対応付けて、その発行権限キーを用いて発行されたＤＩＤやその発行日時の情報を記録している（図５の発行済ＤＩＤリスト）。ＤＩＤサーバ２２０は、検証対象のＤＩＤ６００の発行権限キー６０２と同じ発行権限キーを持つ発行済みＤＩＤの中に、そのＤＩＤ６００中の発行番号６１０と同じ発行番号を持つものがあるかどうかを調べる。そのようなものがあれば、そのＤＩＤ６００は不正なものであると判定される。
【０２０３】
（ｆ）ＤＩＤ６００中の発行年月日６０６及び発行番号６１０の組合せが、そのＤＩＤ６００の発行権限キー６０２と同じ発行権限キーを含む発行済みのＤＩＤの発行年月日と発行番号の組合せと矛盾しないこと。
【０２０４】
ＤＩＤサーバ２２０は、検証対象のＤＩＤ６００の発行年月日６０６と発行番号６１０の組合せが、そのＤＩＤ６００の発行権限キー６０２と同じ発行権限キーを含む個々の発行済ＤＩＤの発行年月日と発行番号の組合せと矛盾するかどうか、すなわち前後関係が逆になっているものがあるかどうか、を判定する。例えばＤＩＤ６００よりも発行年月日が後にもかかわらず、発行番号が小さい発行済みＤＩＤが見つかった場合、ＤＩＤ６００とその発行済みＤＩＤとは矛盾、すなわち前後関係が逆転している。このような矛盾が見つかった場合、検証対象のＤＩＤ６００だけ、あるいはこれとその発行済みＤＩＤとの両方を不正なものと判定する。
【０２０５】

ＤＩＤサーバ２２０は、以上のような基準に従った検証によりあるＤＩＤが不正なものであると判定した場合、その不正なＤＩＤに関連する処理装置１１０の管理者に電子メール等で警告通知を行う。警告通知には、その処理装置１１０の発行したものと偽装したＤＩＤが見つかったことを知らせるメッセージが含まれる。管理者は、その通知により、セキュリティ強化の施策を行う。処理装置１１０の管理者やその連絡先は、処理装置管理サーバ２４０が持つ情報（図６参照）から求めればよい。警告通知の宛先である不正なＤＩＤに関連する処理装置１１０は、そのＤＩＤに含まれる処理装置固有情報６０４が示す処理装置１１０である。また、その不正なＤＩＤに含まれる発行権限キーと同じ発行権限キーを過去に付与したことがある処理装置１１０を警告通知の宛先としてもよい。

【０２０６】

＜ｅＤｏｃの暗号に脆弱性が発見された場合の処理＞

さて、次に、ｅＤｏｃファイルの生成の際の暗号化に用いた暗号化ソフトに脆弱性が発見された場合の処理について説明する。ドキュメント管理システムの運営者は、いずれかの処理装置１１０が用いた暗号化ソフトの特定バージョンに脆弱性が発見されたことを知得した場合、管理システム２００から各処理装置１１０に対して脆弱性通知を送信する。脆弱性通知には、脆弱性が発見された暗号化ソフトのソフト名及びバージョンの情報が含まれる。組織内管理システム１５０が存在する場合には、脆弱性通知は、管理システム２００から組織内管理システム１５０に渡され、組織内管理システム１５０が配下の各処理装置１１０にその脆弱性通知を送信する。この通知に対して、処理装置１１０は図１８に例示する処理を実行する。

【０２０７】

処理装置１１０は、上位装置（管理システム２００又は組織内管理システム１５０）から脆弱性通知を受信（Ｓ２００）すると、その通知が示す脆弱性が見つかった暗号化ソフトのバージョンを用いて自機が暗号化したファイルを特定する（Ｓ２０２）。処理装置１１０のドキュメントＤＢ１１６には、その処理装置１１０が生成した各ｅＤｏｃファイルとそのメタデータが保存されており、それら各ｅＤｏｃファイルのメタデータから各ｅＤｏｃの生成に用いられた暗号化ソフト名とバージョンが分かる（図３に示すメタデータの構造例を参照）。Ｓ２０２では、処理装置１１０は、メタデータに含まれる暗号化ソフト名とバージョンの組合せが、脆弱性通知に示された組合せと一致するｅＤｏｃを特定する。

【０２０８】

次に処理装置１１０は、特定した各ｅＤｏｃファイルを、自機にインストールされている現用の暗号化ソフトのバージョンで再暗号化する（Ｓ２０４）。この例では、処理装置１１０の暗号化ソフトは適切にバージョンアップされており、処理装置１１０が持つ現用の暗号ソフトのバージョンについては脆弱性が未発見であると想定している。一般に、処理装置１１０が過去に用いた暗号化ソフトのバージョンで脆弱性が発見されることが多いと考えられる。なお万が一、脆弱性通知の対象である暗号化ソフトのバージョンが、処理装置１１０の現用バージョンの暗号ソフトである場合には、処理装置１１０は上位装置等から最新バージョンの暗号ソフトをダウンロードし、その最新バージョンを用いて再暗号化を行う。仮に現用の最新バージョンの暗号化ソフトに脆弱性が発見された場合、上位装置は、その脆弱性が解消された更に新しいバージョンの暗号化ソフトを有しているか、そのソフトの配布元の情報を有していると想定できる。再暗号化は、例えば、対象のｅＤｏｃファイルを、そのｅＤｏｃファイルに対応するメタデータに記録されている復号鍵の情報を用いて復号し、その復号結果を新たに生成した暗号鍵を用いて、脆弱性のないバージョンの暗号化ソフトを用いて暗号化する。なお、処理装置１１０の保存するメタデータには復号鍵の情報が、例えば処理装置１１０の公開鍵で暗号化された状態で含まれているものとする（同様に、上位装置に送るメタデータには、その復号鍵がその上位装置の公開鍵で暗号化されたものを含めてもよい）。

【０２０９】

処理装置１１０は、その再暗号化に応じて、そのｅＤｏｃファイルのメタデータを更新

する（Ｓ２０６）。すなわち、メタデータ（図３参照）中のエンコード日時、暗号化情報（暗号化ソフト名、バージョン情報及び鍵情報）を、再暗号化の日時、再暗号化に用いた暗号化ソフト名、バージョン及びその暗号化を解くための復号鍵の情報へと書き換える。そして、処理装置１１０は、更新後のメタデータを保存（例えばそのｅＤｏｃファイルに対する最新のメタデータとして保存）し、上位装置にアップロードする。上位装置は、アップロードされた更新後のメタデータを保存する。

【０２１０】

その後、処理装置１１０は、再暗号化により得られたｅＤｏｃファイルを、メタデータの配信先情報に示される配信先の各閲覧端末１０４に配信するための処理を実行する（Ｓ２０８）。すなわち例えば、配信先の各閲覧端末１０４に対して、配信準備完了通知を送る（図８のステップ（７）参照）。この通知には、ＤＩＤやドキュメント名に加え、配信するｅＤｏｃが既配信のｅＤｏｃの更新版である旨を示す情報を含めてもよい。この配信準備完了通知を受け取った閲覧端末１０４は、閲覧者が閲覧端末１０４のリスト画面５００（図１１参照）で、その再暗号化により配信準備完了通知を受けたｅＤｏｃを閲覧対象に指示した場合、閲覧端末１０４は、その指示に応じて処理装置１１０から取得したｅＤｏｃファイルと、自機内にある再暗号化前のｅＤｏｃファイルに上書きする。また閲覧端末１０４は、そのｅＤｏｃファイルと共に受け取った更新後のメタデータを、そのｅＤｏｃの最新のメタデータとして保存する。これにより、脆弱性のある暗号化ソフトで暗号化されたｅＤｏｃファイル及びそれに対応するメタデータは閲覧端末１０４からなくなり、脆弱性の見つかっていない暗号化ソフトで再暗号化されたｅＤｏｃファイル及びメタデータに置き換えられる。

【０２１１】

なお、処理装置１１０は、再暗号化したｅＤｏｃの閲覧準備完了通知を送る際又はその前に、そのｅＤｏｃのＤＩＤを含む削除通知を配信先の各閲覧端末１０４に明示的に送信してもよい。この場合、その指示に応じて各閲覧端末１０４が、そのＤＩＤを持つ既存のｅＤｏｃファイル（再暗号化前のもの）を削除する。このとき既存のメタデータも併せて削除してもよい。

【０２１２】

＜配信先端末指定の別の例＞

これまでに説明した例では、配信者が作成端末１０２のＵＩ画面（図９の入力画面４００）で選択可能な配信先のユーザ及び閲覧端末１０４は、同じローカルシステム１００内の処理装置１１０に登録されたユーザ及び閲覧端末１０４か、あるいは同じ組織の組織内管理システム１５０に登録されたユーザ及び閲覧端末１０４（この場合、別の処理装置１１０に登録されたユーザ及び閲覧端末１０４も配信先に指定可能）に限られていた。

【０２１３】

しかし、組織内のユーザが組織外の人（ゲスト）を交えた会議において、作成した会議メモ等のドキュメントをゲストに対して一時的に閲覧させたい場合もある。このような場合に、ゲストやゲストの携帯端末を処理装置１１０やその上位装置に登録したり、閲覧終了後にその登録を解除したりするのは煩雑な作業となる。

【０２１４】

そこで、本実施形態では、ゲストの端末と判断できる閲覧端末１０４には、一定の制限の下でｅＤｏｃを配信可能とする。

【０２１５】

例えば、作成端末１０２の近傍にいるユーザの端末はゲスト端末であると見なし、そのゲスト端末を配信先端末選択メニュー４０６の選択肢に加える。あるいは、処理装置１１０の近傍にいるユーザの端末はゲスト端末であると見なし、そのゲスト端末を配信先端末選択メニュー４０６の選択肢に加える。作成端末１０２や処理装置１１０は、組織の建物の部屋（例えば部署の居室、会議室）に設置されていることが多いと考えられ、作成端末１０２又は処理装置１１０の近くにいる人は、会議等のためにしかるべき許可を受けてその部屋に入室している人であると想定される。

【０２１６】
例えば、処理装置１１０又は作成端末１０２は、Bluetooth Low Energy（登録商標）等の近距離無線通信を用いて通信可能な相手端末を探し、見つかった相手端末、又はそれら相手端末のうち自機からの距離（その近距離無線通信には、自機と相手の通信距離を求めることができるものもある）があらかじめ定めた閾値以下の端末を、自機の近傍にあるゲスト端末と判定する。そして、配信先端末選択メニュー４０６には、処理装置１１０又は作成端末１０２が検出したゲスト端末の端末名が、あらかじめ登録されている組織内の閲覧端末１０４とは別の表示態様で、選択肢として表示される。配信者は、その中で、配信先とするゲスト端末を選択可能である。
【０２１７】
ここで、処理装置１１０又は作成端末１０２は、自機の近傍にある端末すべてではなく、それら近傍の端末のうち所定の条件を満たすもののみをゲスト端末として配信先の選択肢に選んでもよい。例えば、端末が搭載しているビューワアプリケーションその他の特定のソフトウエアのバージョンがあるバージョン以上であることを条件としたり、あらかじめ定められている拒否端末リストに含まれないことを条件とすること等が考えられる。
【０２１８】
ゲスト端末を携帯しているユーザは、処理装置１１０やローカルユーザＩＤサーバ１５２等に登録されていないことが一般的と考えられる。そこで処理装置１１０は、ドキュメントの配信先に指定されたゲスト端末から、ｅＤｏｃファイルやメタデータを要求された場合には、ユーザ認証を省略してそれらデータを配信してもよい。また、ゲスト端末に配信するｅＤｏｃのメタデータには、削除条件が満たされたらそのｅＤｏｃファイル及びメタデータをゲスト端末から削除する旨の削除指示を組み込む。削除条件は、例えばそのｅＤｏｃの画面表示が終了した場合、又は、配信時点から所定の許可期間が経過した場合、等である。ゲスト端末は、削除条件が満たされた時点で、そのｅＤｏｃファイル及びメタデータを自端末内から削除する。これにより、ゲスト端末によるｅＤｏｃの漏洩リスクが低減される。
【０２１９】
＜配信先端末以外からの要求に対する対処＞
これまでに説明した例は、配信者が配信先として指定した閲覧端末１０４に対して処理装置１１０がｅＤｏｃ（又はこれに対応する配信準備完了通知）を配信するという、プッシュ型の配信形態であった。
【０２２０】
しかし、別の例として、閲覧端末１０４からの要求に応じて処理装置１１０が保持しているｅＤｏｃのリストを閲覧端末１０４に提供し、その中からユーザが選択した閲覧対象を閲覧端末１０４に配信するという、プル型の配信形態も考えられる。プル型の配信形態の場合、配信先ユーザが、配信先に指定されていない閲覧端末１０４から処理装置１１０にアクセスし、ｅＤｏｃを要求することも考えられる。このような要求があった場合に処理装置１１０が行う対処として、以下のような方式がある。
【０２２１】
（方式１）　処理装置１１０は、閲覧端末１０４からｅＤｏｃの配信要求を受けた場合に、その閲覧端末１０４が、そのｅＤｏｃの最新のメタデータの配信先情報にて配信先とされている閲覧端末に該当するかどうか判定する。そして、該当しないと判定した場合には、そのｅＤｏｃのファイル（本体）もメタデータもその閲覧端末１０４には送信しない。なお、該当すると判定した場合には、更に、その配信要求を行ったユーザ（あるいはそのユーザと閲覧端末１０４の組合せ）が、そのメタデータの配信先情報に含まれているかどうかを判定し、含まれている場合には配信を行い、含まれていない場合には配信を行わないようにしてもよい。
【０２２２】
このように、方式１では、配信者から指定された配信先に該当しない閲覧端末１０４には、ｅＤｏｃ（本体ファイル及びメタデータ）は配信されない。

【０２２３】
（方式２）　この方式では、処理装置１１０は、ｅＤｏｃの配信要求を送ってきた閲覧端末１０４がそのｅＤｏｃのメタデータの配信先情報に規定された配信先の閲覧端末１０４に該当しない場合でも、その要求を発したユーザ（すなわちその閲覧端末１０４を使用しているユーザ）がその配信先情報に配信先として含まれる場合は、ｅＤｏｃの本体ファイル及びメタデータを送信する。ただし、処理装置１１０は、この場合、送信するｅＤｏｃファイル及びメタデータには、保存不可を示すフラグ情報を組み込む。閲覧端末１０４は、保存不可のフラグ情報を含んだｅＤｏｃファイル及びメタデータは、表示はするが、ユーザからの保存指示は受け付けず、ユーザの閲覧が終了すると、それらを保存せずに破棄する。
【０２２４】
なお、配信先に指定されていない閲覧端末１０４に送信したｅＤｏｃファイル及びメタデータをその閲覧端末１０４に保存させない方式に代えて、保存はいったん認めることも考えられる。ただし、この場合、その後再びその閲覧端末１０４がそのｅＤｏｃファイルを開こうとする際、その閲覧端末１０４は処理装置１１０等にそのｅＤｏｃの最新のメタデータを要求（これは閲覧の許可を求める要求である）するが、その要求に応じて処理装置１１０がその閲覧端末１０４と要求したユーザの組合せがそのメタデータの配信先情報に含まれるか判定し、含まれない場合は、閲覧端末１０４にそのｅＤｏｃを削除する指示を送る。閲覧端末１０４は、その指示に応じて、保存しているそのｅＤｏｃファイルとこれに対応するメタデータを削除する。なお、処理装置１１０は、最新のメタデータを要求した閲覧端末１０４に明示的にｅＤｏｃの削除指示を送る代わりに、単にその最新のメタデータを応答してもよい。この場合、閲覧端末１０４が、受け取った最新のメタデータに、自機と現在のユーザの組合せが含まれているか判定し、含まれていない場合には、ｅＤｏｃファイルを開かず、更にその保存しているｅＤｏｃファイルを削除してもよい。
【０２２５】
以上に説明した図１８の例では、再暗号化後のｅＤｏｃファイルは再暗号化前のｅＤｏｃファイルのＤＩＤを引き継いだが、再暗号化後のｅＤｏｃファイルに再暗号化前のｅＤｏｃファイルとは別のＤＩＤを付与してもよい。この場合、処理装置１１０は、配信先の各閲覧端末１０４に対して、再暗号化前のｅＤｏｃファイルのＤＩＤを含んだ明示的な削除指示を送ることで、脆弱性のある再暗号化前のｅＤｏｃファイルが閲覧端末１０４に残らないようにする。また、再暗号化後のｅＤｏｃファイルと再暗号化前のｅＤｏｃファイルとが互いに同じドキュメントに対応するものであることを示す関連付けの情報を、再暗号化後のｅＤｏｃファイルに対応するメタデータ、又は処理装置１１０内（あるいは上位のＤＩＤサーバ２２０、ローカルＤＩＤサーバ１５４内）に記録する。再暗号化後のｅＤｏｃに対応するメタデータに記録する場合には、例えば、そのメタデータに例えば「更新前のＤＩＤ」の項目として、再暗号化前のｅＤｏｃのＤＩＤを含めればよい。
【０２２６】
＜保護済みドキュメントの検索と検索結果の利用＞
次に、このドキュメント保護システムに蓄積された情報に対する検索処理及びその検索の結果を利用したドキュメント保護の更新処理について説明する。
【０２２７】
このドキュメント保護システムにより配信されたドキュメントを検索する場合、ドキュメント自体の内容やドキュメントのメタデータ３００（図３参照）に対する検索条件を入力して検索することがまず考えられる。
【０２２８】
ここで、ｅＤｏｃ（保護済みドキュメント）が生成され配信されるまでの過程には、配信者や配信先ユーザといったユーザや、元のドキュメントからｅＤｏｃを生成する保護処理を実行した処理装置１１０等といった、様々な主体（ユーザや装置）が関連している。ここで主体とは、ドキュメントに関与している人や装置（例えば該ドキュメントを作成、編集、処理、閲覧等した人や装置）のことをいう。このため、ドキュメント検索の目的に

よっては、ｅＤｏｃに関連した主体についての検索条件を用いてドキュメントを特定（すなわちその検索条件を満たすドキュメントを検索）したい場合がある。

【０２２９】

しかし、ｅＤｏｃのメタデータ３００は、あくまでそのｅＤｏｃの属性情報を示すものであり、そのｅＤｏｃに関わった主体（処理装置１１０やユーザ）の属性情報についてはその一部の項目を含む場合もあるがほとんどの項目は含んでいない。このため、ｅＤｏｃの内容やメタデータ３００に対する検索では、そのｅＤｏｃに関連する主体の属性情報に関して自由な検索条件を指定して検索することができない。

【０２３０】

そこで、この例では、処理装置管理サーバ２４０やユーザＩＤサーバ２１０を参照することで、ｅＤｏｃのメタデータ３００に含まれない主体の属性情報項目に関する検索条件を用いて、ｅＤｏｃを検索できるようにする。

【０２３１】

この例では、あくまで一例であるが、図１９に示すように、管理システム２００内に検索サーバ２５０を設ける。検索サーバ２５０は、管理システム２００にアクセス可能な各端末１０６に対して、検索条件入力用のユーザインタフェース画面（検索画面と呼ぶ。例えばウェブページの形態）を提供し、その画面に対して入力された検索条件を用いて、メタデータサーバ２３０や処理装置管理サーバ２４０を検索することで、その検索条件を満たすｅＤｏｃを検索する。図１９では、説明を簡潔にするために、ｅＤｏｃに関連する主体として処理装置１１０のみを考え、主体に関する検索先として、各処理装置１１０の属性情報を保持・管理している処理装置管理サーバ２４０のみを示している。図１９の例におけるドキュメント検索の流れを、図２０のフローチャートも参照しつつ説明する。

【０２３２】

（１）ユーザの指示に応じて、端末１０６は、検索サーバ２５０にアクセスし、検索画面を取得して画面表示する。ユーザは、その検索画面に対して検索条件を入力する（Ｓ３００）。検索画面では、メタデータ３００（図３参照）、及び各主体の属性情報（図１９の例では処理装置管理サーバ２４０が管理する各処理装置１１０のステータス２４４（図６参照））の各項目についての検索条件が入力可能である。例えば、設置場所が「Ａビルディングの４階」であり、エンコード回路のファームウエアバージョンが「バージョン２．０２以下」というように処理装置１１０の属性項目に関する条件のみを検索条件として受け付けてもよい。また、処理装置１１０の属性項目に関する条件と、キーワードやアクセス権限情報等のメタデータ３００の属性項目に関する条件とを組み合わせた検索条件を受け付け可能としてもよい。

【０２３３】

（２）検索サーバ２５０は、ユーザが入力した検索条件を端末１０６から受け取ると、その検索条件の中に、メタデータの属性項目に関する条件以外の条件、すなわち処理装置１１０等といった主体の属性項目に関する条件、が含まれているかどうかを判定する（Ｓ３０２）。

【０２３４】

Ｓ３０２の判定結果がＮｏ（検索条件が、メタデータに関する条件以外の条件を含まない）である場合、検索サーバ２５０は、メタデータサーバ２３０に蓄積されたメタデータ群の中から、その検索条件を満たすメタデータを検索する（Ｓ３０４）。検索サーバ２５０は、Ｓ３０４で検索した各メタデータに含まれる当該メタデータに対応するｅＤｏｃのＤＩＤ（及びそのＤＩＤに対応するｅＤｏｃの書誌情報（例えばドキュメント名や配信者））を、検索結果として端末１０６に提供する。端末１０６はその検索結果を表示する（Ｓ３１０）。なお検索結果の表示には、検索したＤＩＤに代えて、あるいはこれに加えて、そのＤＩＤに対応する保護済みドキュメントのドキュメント名や配信者等の書誌情報を表示してもよい。

【０２３５】

（３）Ｓ３０２の判定結果がＹｅｓの場合、図１９の例では、入力された検索条件には

、処理装置１１０の属性項目に関する条件（「装置条件」と呼ぶ）が含まれる。検索サーバ２５０は、処理装置管理サーバ２４０に対して、その装置条件を満たす処理装置１１０を問い合わせる（Ｓ３０６）。なお、入力された検索条件の中に、ユーザの属性項目に関する条件（「ユーザ条件」と呼ぶ）が含まれる場合には、検索サーバ２５０は、ユーザＩＤサーバ２１０に対してそのユーザ条件を満たすユーザを問い合わせる。

【０２３６】

（４）この問合せを受けた処理装置管理サーバ２４０は、保持している情報（例えばステータス２４４）をその装置条件で検索することで、その装置条件を満たす処理装置１１０を特定する。

【０２３７】

（５）処理装置管理サーバ２４０は、特定した各処理装置１１０の処理装置ＩＤの情報を検索サーバ２５０に回答する。検索サーバ２５０はその回答を受信する。

【０２３８】

検索サーバ２５０は、処理装置管理サーバ２４０から回答された処理装置ＩＤと、入力された検索条件のうちメタデータの項目についての条件とを組み合わせた条件で、メタデータサーバ２３０を検索する（Ｓ３０８）。処理装置ＩＤはメタデータの項目の１つに含まれており、その項目はそのメタデータに対応するｅＤｏｃを生成（すなわち配信）した処理装置を示す。図１９では、このＳ３０８の処理を（６）～（９）の４ステップで構成した場合の例が示されている。以下これら４ステップを説明する。

【０２３９】

（６）検索サーバ２５０は、処理装置管理サーバ２４０から受け取った各処理装置ＩＤを含んだメタデータをメタデータサーバ２３０に問い合わせる。

【０２４０】

（７）メタデータサーバ２３０は、その問合せに応じて、それら各処理装置ＩＤを含んだメタデータを検索し、検索結果のメタデータ群を検索サーバ２５０に回答する。検索サーバ２５０は、回答されたメタデータ群を受信する。

【０２４１】

（８）検索サーバ２５０は、受信したメタデータ群を検索対象として、その中から入力された検索条件のうちメタデータの項目についての条件を満たすメタデータを検索する。

【０２４２】

（９）検索サーバ２５０は、この検索により得られたメタデータからＤＩＤ等の所定の項目を抽出して、検索結果リストを生成し、そのリストを端末１０６に送信する。

【０２４３】

（１０）端末１０６は、その検索結果リストを受信する。

【０２４４】

（１１）端末１０６は、受信した検索結果リストを画面表示する（Ｓ３１０）。

【０２４５】

以上に説明した検索処理において、入力された検索条件に装置条件とユーザ条件の両方が含まれている場合、検索サーバ２５０は、処理装置管理サーバ２４０から回答された処理装置ＩＤを含んだメタデータをメタデータサーバ２３０に問い合わせると共に、ユーザＩＤサーバ２１０から回答されたユーザＩＤを例えば配信先ユーザとして含んだメタデータをメタデータサーバ２３０に問い合わせる。そして、それら問合せにより得られたメタデータ群を、検索条件における装置条件とユーザ条件との組合せ方（ＡＮＤ条件やＯＲ条件）に従って組み合わせることで、検索対象のメタデータ群を構成する。そして、その検索対象メタデータ群から、入力された検索条件のうちメタデータの項目についての条件を満たすメタデータを求め、求めたメタデータのＤＩＤ等の所定の項目を検索結果とする。

【０２４６】

また例えば、入力された検索条件が装置条件に該当するもののみである場合は、図１９のステップ（７）でメタデータサーバ２３０から回答されたメタデータにＤＩＤ等の情報が最終的な検索結果となる。

【０２４７】
次に、図１９の処理の流れの変形例を説明する。この変形例では、処理装置管理サーバ２４０の検索（図１９の（４）、図２０のＳ３０６）において、装置条件を満たす処理装置ＩＤと期間の組合せを検索する。
【０２４８】
図６に例示したように、処理装置管理サーバ２４０は、各処理装置１１０の最新のステータスだけでなく、過去の個々の更新時点でのステータス２４４の集まりであるステータス履歴２４２を蓄積している。このため、装置条件を満たすステータス２４４を持っている処理装置１１０の処理装置ＩＤだけでなく、ステータス履歴２４２からそのステータス２４４の日時（設定更新等により処理装置１１０のステータス内容がそのステータス２４４となった日時）も求められる。その日時から、その処理装置１１０の次のステータス更新日時までが、装置条件を満たすとして検索されたステータスが有効であった期間である。この変形例では、処理装置管理サーバ２４０は、図１９で説明したステップ（４）で、装置条件を満たすステータス２４４を検索し、そのステータス２４４を含むステータス履歴２４２に含まれる処理装置ＩＤと、そのステータス２４４の日時から、その処理装置の次のステータス２４４の日時までの期間と、を検索結果として求め、検索サーバ２５０に回答する。
【０２４９】
この回答を受けた検索サーバ２５０は、図１９のステップ（６）で、その回答に含まれる処理装置ＩＤと期間の組合せに該当するメタデータを問い合わせる。これに応じ、メタデータサーバ２３０は、その処理装置ＩＤを含み、かつ、エンコード日時（図３参照）がその期間内に該当するメタデータを検索し、その検索の結果を検索サーバ２５０に返す。以降の処理は、図１９に例示したものと同様でよい。
【０２５０】
この変形例によれば、過去のある時点乃至期間にあるステータスを持つ処理装置１１０で生成された保護済みドキュメント（あるいはそのような保護済みドキュメントのうち他の条件を更に満たすもの）が検索可能になる。
【０２５１】
次に、図２１を参照して、検索に関する更なる変形例を説明する。図２１の手順のうちＳ３００～Ｓ３０８までは図２０の手順の同一符号のステップと同様であり、Ｓ３１２以降が図２０の手順と異なる。
【０２５２】
図２１の手順では、検索サーバ２５０は、Ｓ３０４又はＳ３０８により検索条件を満たすメタデータが得られると、それら個々のメタデータに含まれるＤＩＤと処理装置ＩＤの組合せを求める（Ｓ３１２）。そして、求めた組合せ毎に、その組合せに含まれる処理装置ＩＤの処理装置１１０に対して、その組合せに含まれるＤＩＤを持つドキュメントの再暗号化を指示する（Ｓ３１４）。この指示を受けた処理装置１１０は、図１８に示した手順のＳ２０４以降と同様の処理を行えばよい。すなわち、その指示に含まれるＤＩＤに対応する保護済みドキュメントを復号して元のドキュメントを再生し（あるいはそのＤＩＤに対応付けて保存している元のドキュメントを取り出し）、その元のドキュメントを、現在その処理装置１１０にインストールされている最新の暗号ソフトを用いて再び暗号化する（Ｓ２０４）。そして、メタデータを更新し（Ｓ２０６）、その暗号化により生成された新たなｅＤｏｃを各配信先の閲覧端末１０４に配信する（Ｓ２０８）。
【０２５３】
この図２１の手順は、例えば、処理装置１１０が特定のステータスを持つときの暗号化処理に脆弱性が発見された場合に、そのステータスを持つ処理装置１１０で暗号化され生成された保護済みドキュメントを特定し、脆弱性を解消するために用いられる。
【０２５４】
具体例でいえば、例えば、バージョンＸのＯＳ（オペレーティングシステム）で、エンコードソフトＡのバージョンＹを用い、かつ暗号化ソフトＢのバージョンＺを用いた処理

装置１１０の暗号化に脆弱性が見つかったとする。ＯＳのバージョンがＸであり、エンコードソフトの名称がＡでバージョンがＹであり、暗号化ソフトの名称がＢでバージョンがＺである、という組合せは、処理装置１１０のステータスの一部を構成する。管理システム１５０の管理者は、そのようなステータスの処理装置１１０で暗号化され配信されたｅＤｏｃを特定し、そのｅＤｏｃを安全な条件で再暗号化して配信し直す必要があると判断する。この場合、管理者は、上述したＯＳ、エンコードソフト、暗号化ソフトのステータス項目の組合せを装置条件として含む検索条件を検索サーバ２５０に入力する。検索サーバ２５０は、図２１の手順に従って、その検索条件に該当するｅＤｏｃのＤＩＤと処理装置１１０のＩＤを特定し、そのｅＤｏｃの再暗号化（及び再配信）をその処理装置１１０に指示する。

【０２５５】

図２１の例は、検索条件を満たすｅＤｏｃを処理装置１１０に再暗号化させるものであったが、再暗号化以外の別の再処理を処理装置１１０に実行させるために、図２１と同様の手順を用いてもよい。

【０２５６】

例えば、組織の部署の統合により廃止される部署が発生し、その部署に属しているユーザに配信した特定のｅＤｏｃについてのアクセス権限を変更（例えば統合先の部署に対応したアクセス権限内容に変更）する必要がでてきた場合を考える。この場合、その条件に該当するｅＤｏｃを特定し、そのｅＤｏｃに設定されているアクセス権限情報（図３のメタデータ３００参照）を、新たな内容に再設定する処理を行うこととなる。この場合管理者は、その部署をユーザ条件として含む検索条件を検索サーバ２５０に入力する。検索サーバ２５０は、その検索条件に含まれるユーザ条件が示す部署に属するユーザをユーザＩＤサーバ２１０に問い合わせる。検索サーバ２５０は、この問合せにより得られたユーザＩＤを配信先情報に含むメタデータをメタデータサーバ２３０に問い合わせる。そして、検索サーバ２５０は、この問合せに対してメタデータサーバ２３０から回答されたメタデータのからＤＩＤと処理装置ＩＤを抽出する。そして、その処理装置ＩＤに対応する処理装置１１０に対して、そのＤＩＤに対応するメタデータのアクセス権限情報を、所定の内容（これは管理者が検索サーバ２５０に指示すればよい）に更新するよう指示する。この指示を受けた処理装置１１０は、その指示に応じてそのメタデータを更新し、この更新を上位装置（組織内メタデータサーバ１５６やメタデータサーバ２３０）に通知する。

【０２５７】

また、廃止される部署に所属していたユーザに配信したｅＤｏｃについて、そのユーザをそのｅＤｏｃの配信先から外したい場合にも、図２１の手順が利用可能である。すなわち、検索サーバ２５０は、管理者から入力された検索条件（部署）に応じて、その部署に所属していたユーザを検索し、検索したユーザに配信したｅＤｏｃを特定する（Ｓ３１２）。そして、特定したｅＤｏｃを生成した処理装置１１０に対して、そのｅＤｏｃの配信先からそれら検索したユーザを削除してｅＤｏｃの再生成（すなわち異なる暗号鍵を用いて再暗号化し、それら検索したユーザを削除した残りの配信先ユーザを配信先情報に記したメタデータを生成）及び再配信（残りの配信先ユーザへの配信）を指示する。このとき、配信先から削除されたユーザに対して、そのｅＤｏｃ（再生成前のもの）を削除する指示を送信するよう、その処理装置１１０に指示してもよい。

【０２５８】

以上、本発明の実施形態を説明した。以上に例示した作成端末１０２、閲覧端末１０４、処理装置１１０、ローカルユーザＩＤサーバ１５２、ローカルＤＩＤサーバ１５４、ローカルメタデータサーバ１５６、ユーザＩＤサーバ２１０、ＤＩＤサーバ２２０、メタデータサーバ２３０、処理装置管理サーバ２４０等の各装置は、コンピュータに上述のそれら各装置の機能を表すプログラムを実行させることにより実現される。ここで、コンピュータは、例えば、ハードウエアとして、ＣＰＵ等のマイクロプロセッサ、ランダムアクセスメモリ（ＲＡＭ）およびリードオンリメモリ（ＲＯＭ）等のメモリ（一次記憶）、フラッシュメモリやＳＳＤ（ソリッドステートドライブ）、ＨＤＤ（ハードディスクドライブ

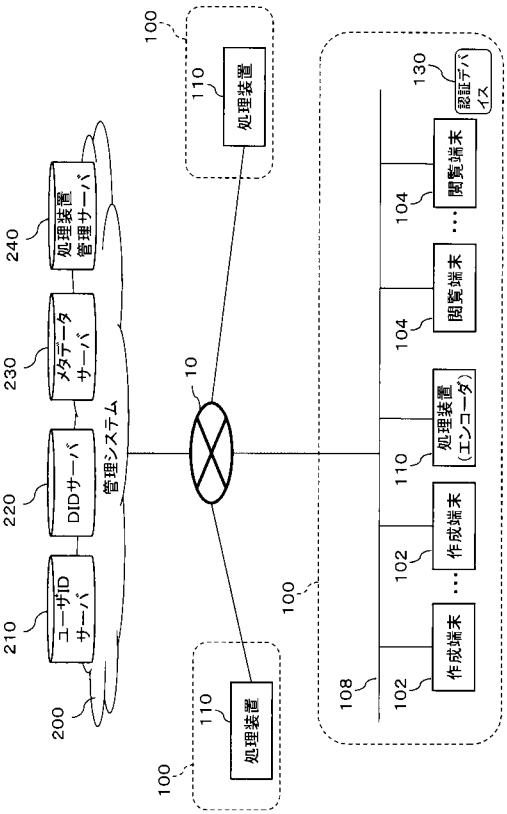
）や等の固定記憶装置を制御するコントローラ、各種Ｉ／Ｏ（入出力）インタフェース、ローカルエリアネットワークなどのネットワークとの接続のための制御を行うネットワークインタフェース等が、たとえばバス等を介して接続された回路構成を有する。それら各機能の処理内容が記述されたプログラムがネットワーク等の経由でフラッシュメモリ等の固定記憶装置に保存され、コンピュータにインストールされる。固定記憶装置に記憶されたプログラムがＲＡＭに読み出されＣＰＵ等のマイクロプロセッサにより実行されることにより、上に例示した機能モジュール群が実現される。

【符号の説明】

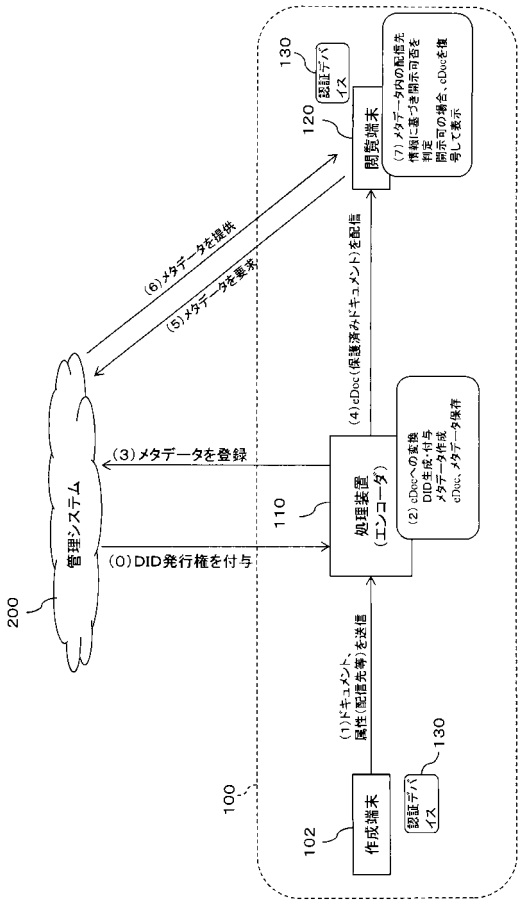
【０２５９】

１０　広域ネットワーク、１００　ローカルシステム、１０２　作成端末、１０４　閲覧端末、１０８　ローカルネットワーク、１１０　処理装置、１１２　管理情報記憶部、１１２ａ　管理情報、１１４ａ　ユーザ情報、１３０　認証デバイス、１５０　組織内管理システム、１５２　ローカルユーザＩＤサーバ、１５４　ローカルＤＩＤサーバ、１５６　ローカルメタデータサーバ、２００　管理システム、２１０　ユーザＩＤサーバ、２１２　契約者データ、２１４　一般ユーザデータ、２２０　ＤＩＤサーバ、２３０　メタデータサーバ、２４０　処理装置管理サーバ、２４２　ステータス履歴、２４４　ステータス、２４６　ソフトウエア情報、２４８　ハードウエア情報、３００　メタデータ、４００　入力画面、４０２　配信先ユーザ選択メニュー、４０４　配信先ユーザリスト欄、４０６　配信先端末選択メニュー、４０８　配信先端末リスト欄、４１０　アクセス権限設定欄、４１２　オフライン有効期間メニュー、４１４　オプション設定呼出ボタン、４２０　オプション設定画面、４２２　処理装置指定欄、４２４　元データ設定欄、５００　リスト画面、５０２　通知マーク、５０４　ドキュメント名、５０６　閲覧可否マーク、６０２　発行権限キー、６０４　処理装置固有情報、６０６　発行年月日、６０８　発行証明キー、６１０　発行番号。

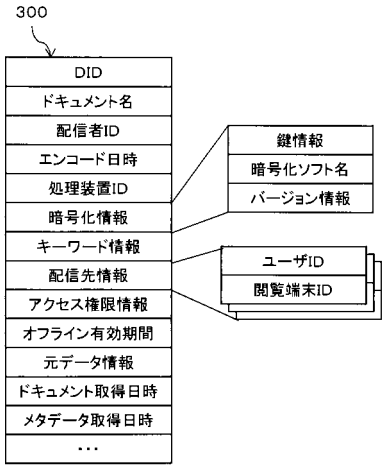
【図１】



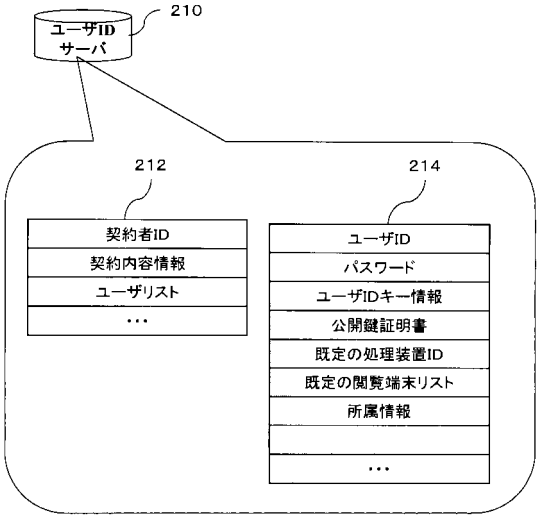
【図２】



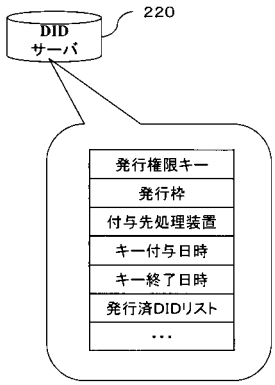
【図３】


300
DID
ドキュメント名
配信者ID
エンコード日時
処理装置ID
暗号化情報
キーワード情報
配信先情報
アクセス権限情報
オフライン有効期間
元データ情報
ドキュメント取得日時
メタデータ取得日時
…
鍵情報
暗号化ソフト名
バージョン情報
ユーザID
閲覧端末ID

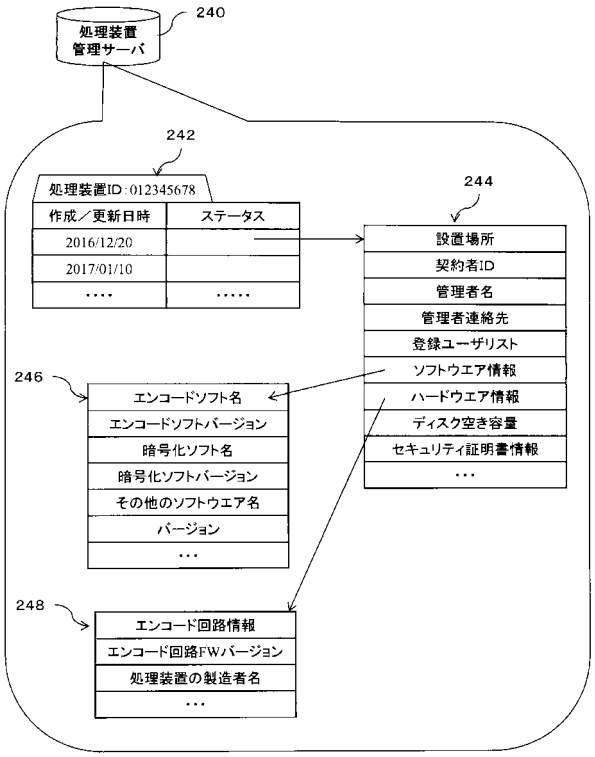
【図４】


210
ユーザID
サーバ
212
契約者ID
契約内容情報
ユーザリスト
…
214
ユーザID
パスワード
ユーザIDキー情報
公開鍵証明書
既定の処理装置ID
既定の閲覧端末リスト
所属情報
…

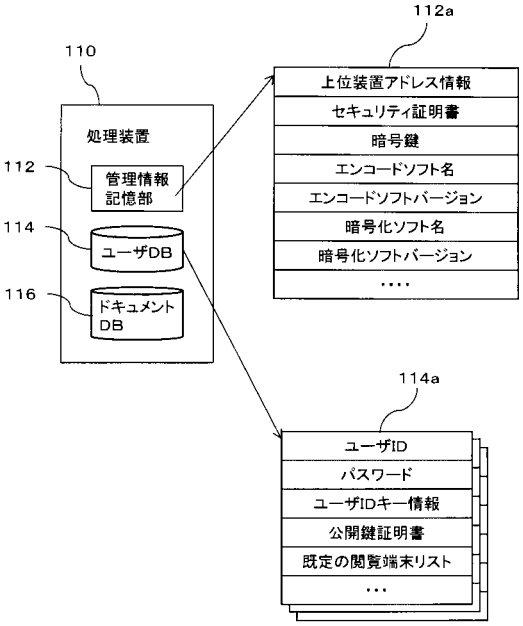
【図５】


220
DID
サーバ
発行権限キー
発行枠
付与先処理装置
キー付与日時
キー終了日時
発行済DIDリスト
…

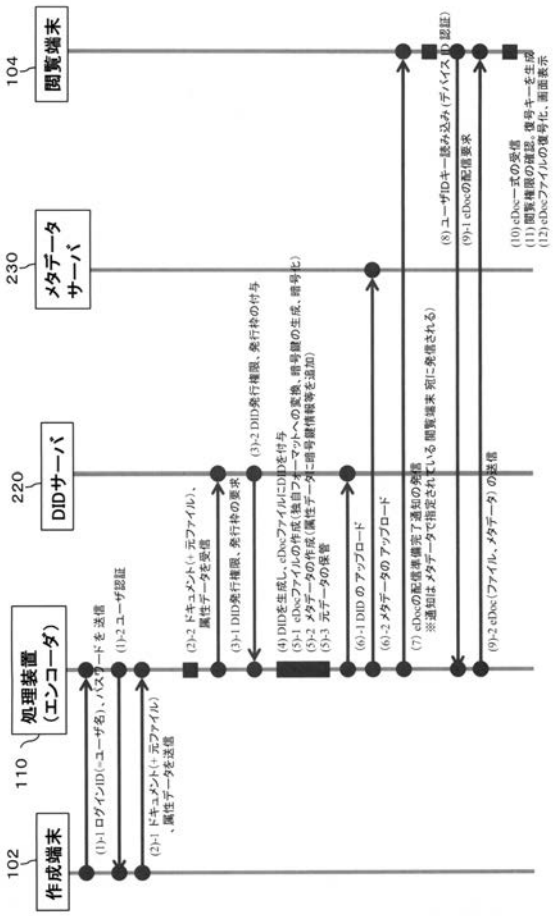
【図６】


240
処理装置
管理サーバ
242
処理装置ID：012345678
作成／更新日時
ステータス
2016/12/20
2017/01/10
244
設置場所
契約者ID
管理者名
管理者連絡先
登録ユーザリスト
ソフトウエア情報
ハードウエア情報
ディスク空き容量
セキュリティ証明書情報
…
246
エンコードソフト名
エンコードソフトバージョン
暗号化ソフト名
暗号化ソフトバージョン
その他のソフトウエア名
バージョン
…
248
エンコード回路情報
エンコード回路FWバージョン
処理装置の製造者名
…

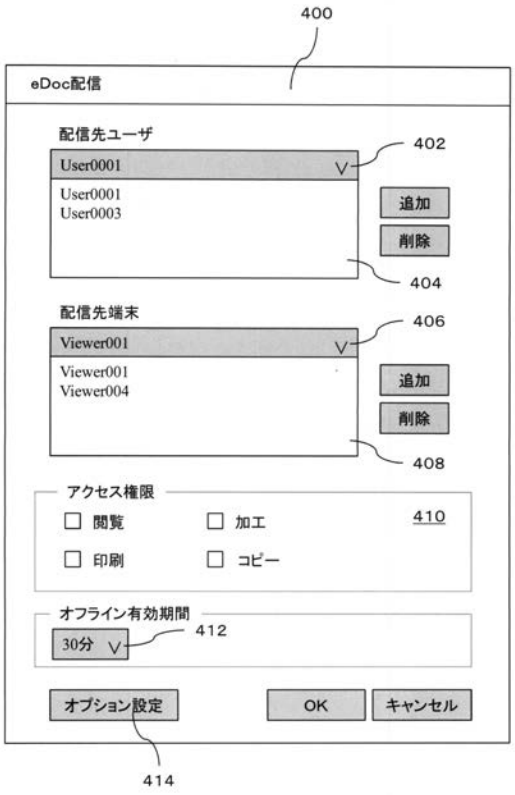
【図７】


110
処理装置
112
管理情報記憶部
114
ユーザDB
116
ドキュメントDB
112a
上位装置アドレス情報
セキュリティ証明書
暗号鍵
エンコードソフト名
エンコードソフトバージョン
暗号化ソフト名
暗号化ソフトバージョン
....
114a
ユーザID
パスワード
ユーザIDキー情報
公開鍵証明書
既定の閲覧端末リスト
...

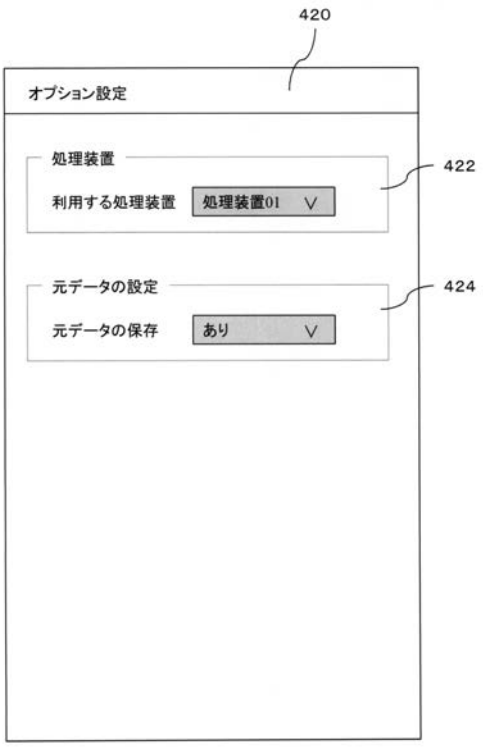
【図８】


104 閲覧端末
230 メタデータサーバ
220 DIDサーバ
処理装置（エンコーダ）
110
102 作成端末
(1)-1 ログインID(ユーザ名)、パスワードを送信
(1)-2 ユーザ認証
(2)-1 ドキュメント(+元ファイル)、属性データを送信
(2)-2 ドキュメント(+元ファイル)、属性データを受信
(3)-1 DID発行権限、発行枠の要求
(3)-2 DID発行権限、発行枠の付与
(4) DIDを生成し、eDocファイルにDIDを付与
(5)-1 eDocファイルの作成(独自フォーマットへの変換、暗号鍵の生成、暗号化)
(5)-2 メタデータの作成(属性データ+暗号鍵情報等を追加)
(5)-3 元データの保管
(6)-1 DID のアップロード
(6)-2 メタデータのアップロード
(7) eDocの配信準備完了通知の発信
※通知はメタデータで指定されている閲覧端末 宛に発信される
(8) ユーザIDキー読み込み(デバイス)、認証
(9)-1 eDocの配信要求
(9)-2 eDoc(ファイル、メタデータ)の送信
(10) eDoc一式の受信
(11) 閲覧権限の確認、復号キーを生成
(12) eDocファイルの復号化、画面表示

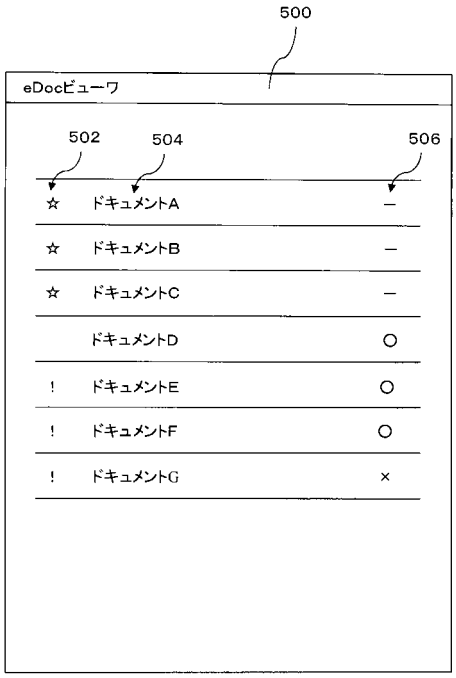
【図９】


400
eDoc配信
配信先ユーザ
User0001
User0001
User0003
402
追加
削除
404
配信先端末
Viewer001
Viewer001
Viewer004
406
追加
削除
408
アクセス権限
閲覧
加工
印刷
コピー
410
オフライン有効期間
30分
412
オプション設定
OK
キャンセル
414

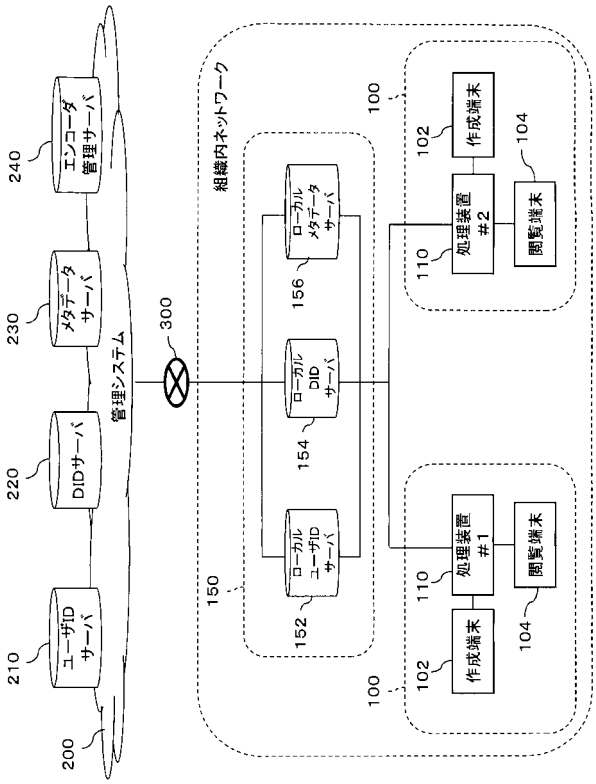
【図１０】


420
オプション設定
処理装置
利用する処理装置
処理装置01
422
元データの設定
元データの保存
あり
424

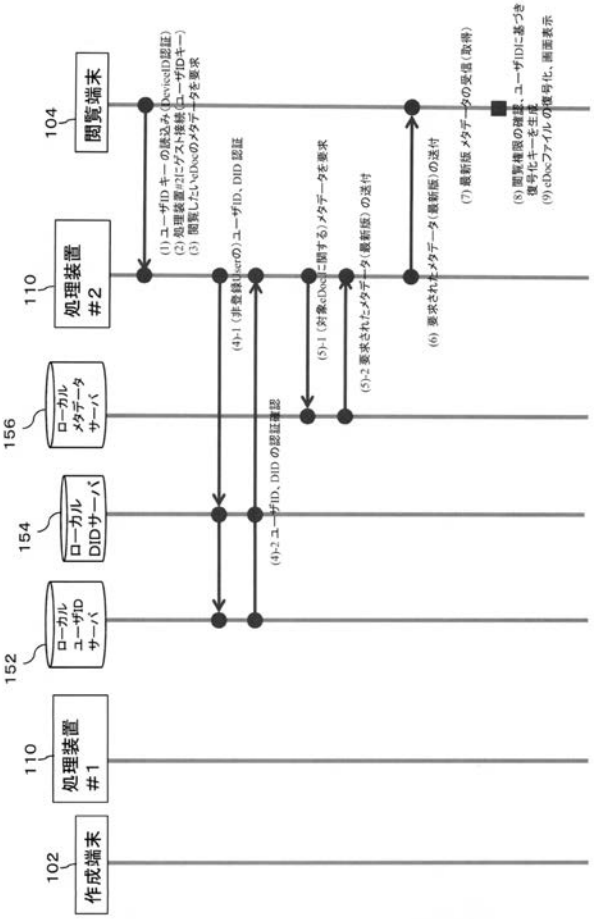
【図１１】



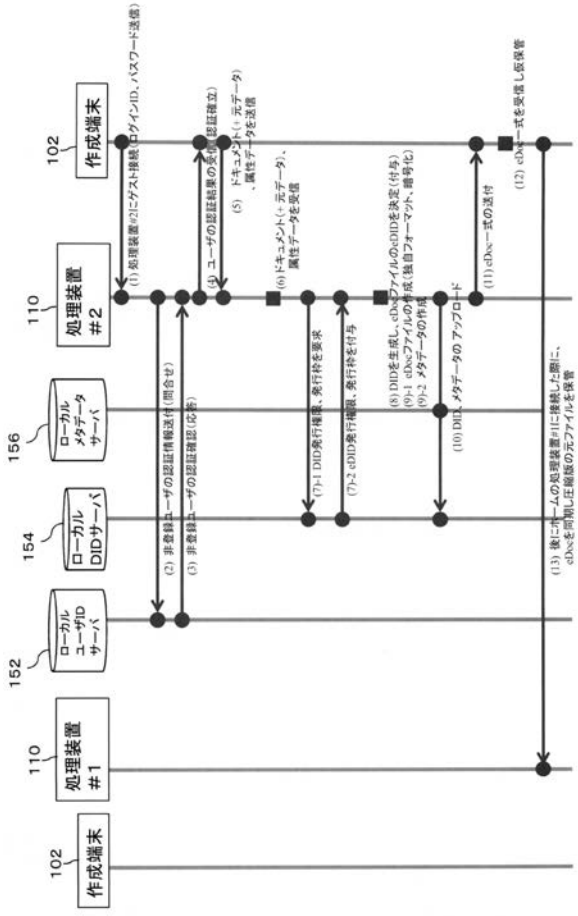
【図１２】



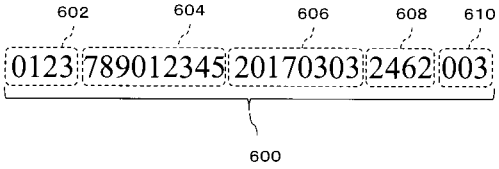
【図１３】



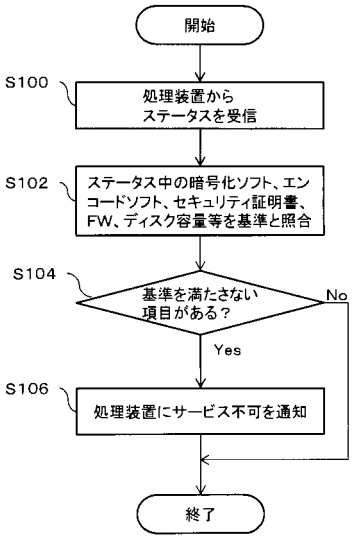
【図１４】



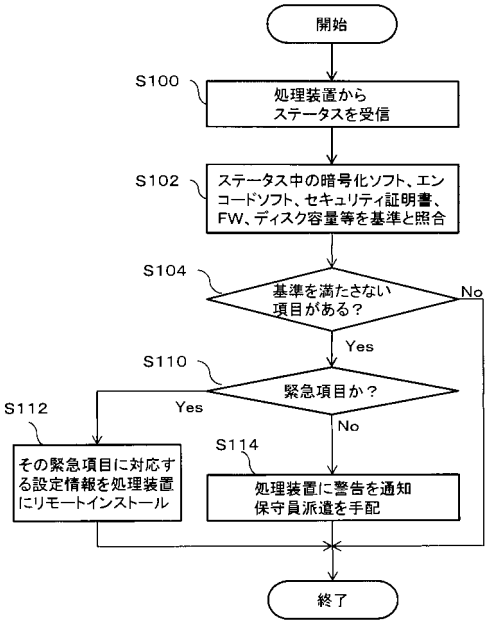
【図１５】



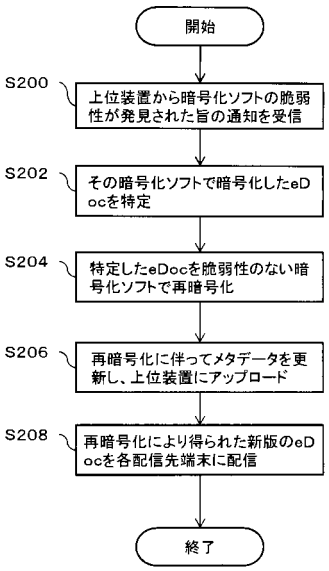
【図１６】



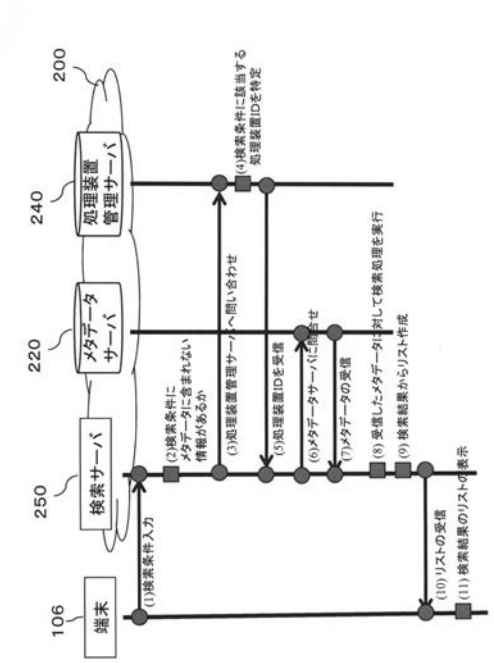
【図１７】



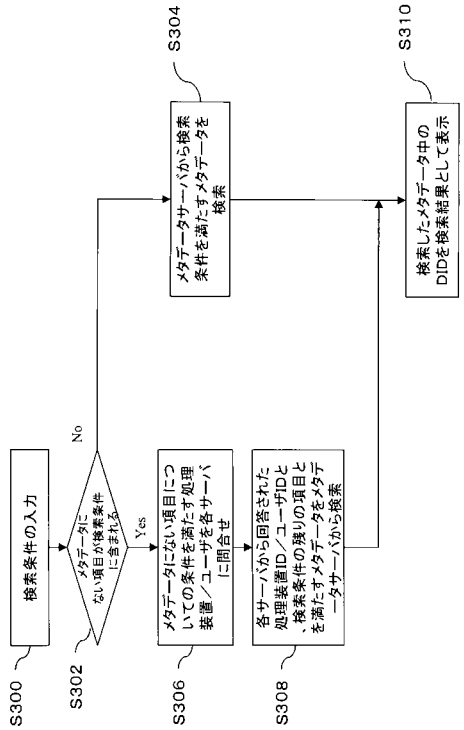
【図１８】



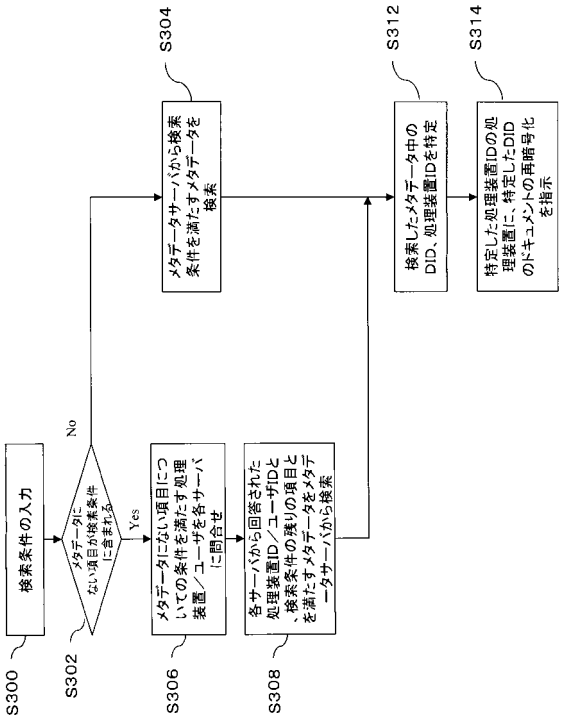
【図１９】



【図２０】


検索条件の入力
メタデータに
ない項目が検索条件
に含まれる
No
Yes
メタデータサーバから検索
条件を満たすメタデータを
検索
メタデータにない項目につ
いての条件を満たす処理
装置／ユーザを各サーバ
に問合せ
各サーバから回答された
処理装置ID／ユーザIDと
、検索条件の残りの項目と
を満たすメタデータをメタデ
ータサーバから検索
検索したメタデータ中の
DIDを検索結果として表示
S300
S302
S304
S306
S308
S310

【図２１】


検索条件の入力
メタデータに
ない項目が検索条件
に含まれる
No
Yes
メタデータサーバから検索
条件を満たすメタデータを
検索
メタデータにない項目につ
いての条件を満たす処理
装置／ユーザを各サーバ
に問合せ
各サーバから回答された
処理装置ID／ユーザIDと
、検索条件の残りの項目と
を満たすメタデータをメタデ
ータサーバから検索
検索したメタデータ中の
DID、処理装置IDを特定
特定した処理装置IDの処
理装置に、特定したDID
のドキュメントの再暗号化
を指示
S300
S302
S304
S306
S308
S312
S314