(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2007-280181
(P2007-280181A)
(43)公開日　平成19年10月25日(2007.10.25)

(51)Int.Cl.		F I		テーマコード（参考）
G06Q 10/00	(2006.01)	G06F 17/60	162C	5B009
G06F 17/21	(2006.01)	G06F 17/21	570M	5B017
G06F 21/24	(2006.01)	G06F 17/60	512	
		G06F 12/14	540A	
		G06F 12/14	520A	

審査請求 未請求　請求項の数 14　OL　（全 19 頁）　最終頁に続く

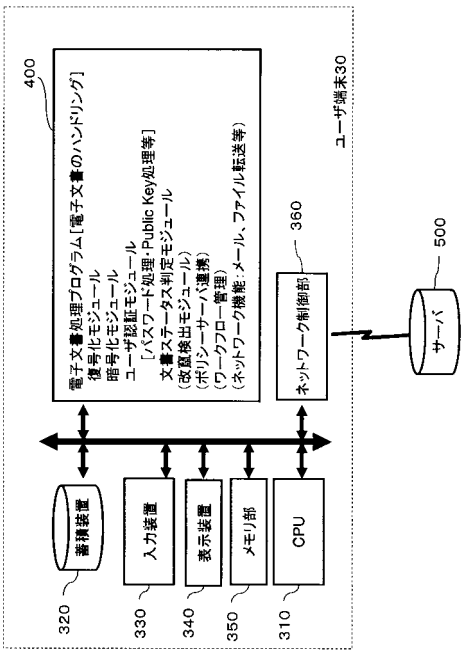
(21)出願番号　特願2006-107484 (P2006-107484)
(22)出願日　平成18年4月10日 (2006.4.10)

(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　100075258
弁理士　吉田　研二
(74)代理人　100096976
弁理士　石田　純
(72)発明者　窪寺　隆行
神奈川県川崎市高津区坂戸３丁目２番１号
ＫＳＰ　Ｒ＆Ｄ　ビジネスパークビル
富士ゼロックス株式会社内

Fターム(参考)　5B009 SA14　TB13　VC03
5B017 AA03　AA08　BA06　BA07　BA09
CA16

(54)【発明の名称】電子文書の処理プログラム及び電子文書の処理装置

(57)【要約】
【課題】複数のユーザ間で受け渡される電子文書の項目毎の機密維持を図る。
【解決手段】複数の項目を有するフォームを備える電子文書では、項目がそれぞれ別のオブジェクトとして定義され、項目への入力データが、オブジェクト毎又は同一グループと分類されたオブジェクトのグループ毎に異なる鍵を用いて暗号化された暗号化データの格納部と、オブジェクト又はグループ毎に、暗号化データを権限あるユーザに復号化するための復号化情報を格納する復号化情報の格納部とを備える。この電子文書を処理する際、ユーザ権限を判定し、復号化情報に基づき、該ユーザに閲覧権限が与えられたオブジェクト又はグループのみ暗号化データを復号化する。よって、後で処理するユーザに対しても、入力済みの全データを閲覧させずに作業させることができ項目毎の機密性維持ができる。
【選択図】図２



【特許請求の範囲】
【請求項１】
複数の項目を有するフォームを備える電子文書の処理プログラムであって、
前記電子文書は、
前記複数の項目がそれぞれ別のオブジェクトとして定義され、
オブジェクト毎に異なる鍵、又は同一グループとして分類されたオブジェクトのグループ毎に異なる鍵を用いて、各項目に入力されたデータを暗号化して得る暗号化データの格納部と、
前記オブジェクト毎又は前記グループ毎に、前記暗号化データを権限あるユーザに対して復号化するための復号化情報を格納する復号化情報の格納部と、を備え、
コンピュータに、
各ユーザに与えられた権限を判定する判定処理、
所定のユーザが前記電子文書を開いた際、前記復号化情報に基づいて、該ユーザに閲覧権限が与えられた前記オブジェクト毎又は前記グループ毎に暗号化データを復号化する復号化処理、
を実行させることを特徴とする電子文書の処理プログラム。
【請求項２】
請求項１に記載の電子文書の処理プログラムにおいて、
前記復号化情報は、オブジェクト毎又はグループ毎に、ユーザ識別情報と、ユーザ権限情報とを備え、
コンピュータに、
該電子文書に格納されている前記ユーザ識別情報及び前記ユーザ権限情報とに基づいて、前記電子文書を開いたユーザに対する権限を判定させ、
前記電子文書を開いたユーザが閲覧権限を持たない前記オブジェクト又は前記グループについて、暗号化データが存在する場合、コンピュータモニタに対し、対応する項目には格納されている該暗号化データ又は該暗号化データに代えて任意の判読不能なデータを表示させ、又は項目を非表示とさせ、
前記電子文書を開いたユーザが閲覧権限を持つ場合には、該当する暗号化データを復号化させ、
得られた復号化データを対応する項目のデータとして前記コンピュータモニタに表示させることを特徴とする電子文書の処理プログラム。
【請求項３】
請求項１又は請求項２に記載の電子文書の処理プログラムにおいて、
コンピュータに、
さらに、前記ユーザが入力権の設定された前記項目に入力したデータを、該データを該当する項目の前記オブジェクト毎又は前記グループ毎の鍵によって暗号化する暗号化処理と、
前記電子文書の暗号化データの格納部に格納する格納処理と、を実行させることを特徴とする電子文書の処理プログラム。
【請求項４】
請求項３に記載の電子文書の処理プログラムにおいて、
コンピュータに、
前記ユーザに対して復号化されたデータを、該当する項目の前記オブジェクト毎又は前記グループ毎の鍵によって暗号化する暗号化処理を実行させることを特徴とする電子文書の処理プログラム。
【請求項５】
請求項３又は請求項４に記載の電子文書の処理プログラムにおいて、
前記電子文書の前記オブジェクトには、該オブジェクトが属するとして分類されたグループのグループ識別情報が付されており、
コンピュータに、

前記入力されたデータを暗号化するための前記鍵として、前記グループ識別情報毎に設定された鍵を用いて暗号化処理を実行させることを特徴とする電子文書の処理プログラム。

【請求項６】

請求項５に記載の電子文書の処理プログラムにおいて、

前記電子文書は前記グループ識別情報と、該グループに属するオブジェクトとの参照テーブルを有し、

コンピュータに、

前記電子文書をユーザが開いた際、前記参照テーブルを参照して、該ユーザに与えられた権限に応じた前記オブジェクト又は前記グループを判別させ、

前記ユーザが閲覧権限のある前記オブジェクト又は前記グループの暗号化データを復号化させることを特徴とする電子文書。

【請求項７】

請求項１～請求項６のいずれか一項に記載の電子文書の処理プログラムにおいて、

コンピュータに、

該電子文書の前記各項目における入力データの有無を判定させ、

該データの有無に応じて、前記オブジェクト毎又は前記グループ毎のユーザ権限を設定することを特徴とする電子文書の処理プログラム。

【請求項８】

請求項７に記載の電子文書の処理プログラムにおいて、

前記電子文書は、前記各項目における入力データの有無から、該電子文書のステータスを判定するステータス判定部を備えており、

前記電子文書が開かれる際、コンピュータに、該ステータス判定部での判定を実行させ、

判定されたステータスに応じて、前記オブジェクト毎又は前記グループ毎にユーザの権限を設定させることを特徴とする電子文書の処理プログラム。

【請求項９】

請求項８に記載の電子文書の処理プログラムにおいて、

前記電子文書は、前記ステータス判定部に対する改竄を検証するための改竄防止情報を備え、

コンピュータに、

該改竄防止情報に基づいて該電子文書を開くかどうかを決定させることを特徴とする電子文書の処理プログラム。

【請求項１０】

請求項１～請求項９のいずれか一項に記載の電子文書の処理プログラムにおいて、

ポリシー管理サーバの管理環境下で前記電子文書が開かれる場合には、前記電子文書のオブジェクト毎又はオブジェクトグループ毎のユーザの権限を、該ポリシー管理サーバによって管理可能とさせることを特徴とする電子文書の処理プログラム。

【請求項１１】

複数の項目を有するフォームを備える電子文書の処理装置であって、

前記電子文書は、

前記複数の項目がそれぞれ別のオブジェクトとして定義され、

オブジェクト毎に異なる鍵、又は同一グループとして分類されたオブジェクトのグループ毎に異なる鍵を用いて、各項目に入力されたデータを暗号化して得る暗号化データの格納部と、

前記オブジェクト毎又は前記グループ毎に、前記暗号化データを権限あるユーザに対して復号化するための復号化情報を格納する復号化情報の格納部と、を備え、

該電子文書の処理装置は、

各ユーザに与えられた権限を判定するユーザ権限判定手段と、

所定のユーザが前記電子文書を開いた際、前記復号化情報に基づいて、該ユーザに閲覧

権限が与えられた前記オブジェクト毎又は前記グループ毎に暗号化データを復号化する復号化手段と、
を備えることを特徴とする電子文書の処理装置。
【請求項１２】
請求項１１に記載の電子文書の処理装置において、
前記復号化情報は、オブジェクト毎又はグループ毎に、ユーザ識別情報と、ユーザ権限情報とを備え、
前記ユーザ権限判定手段は、該電子文書に格納されている前記ユーザ識別情報及び前記ユーザ権限情報とに基づいて、前記電子文書を開いたユーザに対する権限を判定し、
前記電子文書を開いたユーザが閲覧権限を持たない前記オブジェクト又は前記グループについて、暗号化データが存在する場合、モニタに対し、対応する項目には格納されている該暗号化データ又は該暗号化データに代えて任意の判読不能なデータを表示させ、又は項目を非表示とさせ、
前記電子文書を開いたユーザが閲覧権限を持つ場合、
前記復号化手段が、該当する暗号化データを復号化し、
得られた復号化データを対応する項目のデータとして前記モニタに表示することを特徴とする電子文書の処理装置。
【請求項１３】
請求項１１又は請求項１２に記載の電子文書の処理装置において、
さらに、前記ユーザが入力権の設定された前記項目に入植したデータを、該データを該当する項目のオブジェクト毎又はグループ毎の鍵によって暗号化する暗号化手段と、
コンピュータに、
さらに、前記ユーザが入力権の設定された前記項目に入植したデータを、該データを該当する項目のオブジェクト毎又はグループ毎の鍵によって暗号化する暗号化処理と、
前記電子文書の暗号化データの格納部に格納する格納処理を実行することを特徴とする電子文書の処理装置。
【請求項１４】
請求項１３に記載の電子文書の処理装置において、
前記暗号化手段は、前記ユーザに対して復号化されたデータを、該当する項目のオブジェクト毎又はグループ毎の鍵によって暗号化することを特徴とする電子文書の処理プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
ワークフローにおいて複数のユーザ間で受け渡される電子文書の機密管理に関する。
【背景技術】
【０００２】
従来より電子文書に対して、ネットワークを利用して複数のユーザがそれぞれデータ入力、審査、承認などを実行するワークフローが知られている。このようなワークフローにおいて電子文書の機密性管理が求められる場合には、文書全体を暗号化して電子文書を直接ネットワークを介して受け渡すなどの方法の他、サーバの管理下のデータベースに電子文書を保管してユーザにアクセスさせる方法が知られている。
【０００３】
例えば、特許文献１では、フォームが設定されている電子文書の処理にあたり、ワークフロー情報、フォーム情報、入力データ情報等を保管するデータベースに対し、サーバの管理の下に、ユーザがクライアントコンピュータからサーバを介してデータベースにアクセスするシステムが開示されている。さらに、特許文献１では、ワークフロー情報に応じて、アクセスしたユーザに対し、該当ユーザに必要な情報のみを表示し、また、入力を受け付けるシステムを採用し、作業効率の向上を図っている。
【０００４】

また、特許文献２においても、サーバ（ここでは文書交換サーバ）が、ユーザ間で取り交わす電子文書（ドキュメント）を保管するデータベース、ユーザＩＤ、アクセス権限等のワークフロー情報を保管するデータベースを管理し、サーバがワークフロー情報を参照して各ユーザのデータベースへのアクセスが行われるシステムが開示されている。特許文献２では、サーバがデータベースに保管する電子文書と、その電子文書についての処理ルートやアクセス権限などのワークフロー情報と１対１でリンクさせることで、電子文書毎のアクセス権などを設定することが可能となっている。

【０００５】

さらに、特許文献３においても、電子文書に対するユーザのアクセス権限を管理するサーバを備え、電子文書及びユーザ識別情報などのデータはサーバ管理下のデータベースに保管されている。この特許文献３では、いわゆる電子メールシステムなどを利用して電子文書の配信を行う場合、サーバが、受信者（ユーザ情報）と受信順序及び配信すべき電子文書を管理し、設定された受信順序でユーザに電子文書へのアクセスを許可する。受信順序の後に設定されたユーザに対して、予め設定された範囲で電子文書の一部の情報の閲覧を可能としたり、受信順序の前のユーザが設定期間内に処理を実行しない場合、サーバが代理ユーザを探し、この代理ユーザが電子文書にアクセスした後に、当初から設定されていた次のユーザに対して電子文書へのアクセスが許可することも開示されている。

【０００６】

【特許文献１】特開２００１－２６５９１６号

【特許文献２】特開２００５－１３５０７２号

【特許文献３】特開平１１－５３４５６号

【発明の開示】

【発明が解決しようとする課題】

【０００７】

以上のように電子文書を処理するワークフローを形成する場合、上記特許文献１から３等に開示されているように、サーバが電子文書及びアクセス権限などを管理することで、電子文書の機密管理が可能となる。

【０００８】

しかし、このような従来システムでは、ワークフローの管理サーバにアクセスできないようなオフライン環境などにおいては、電子文書に対する作業ができないことになる。また、例えば特許文献２にも開示されているように、ユーザ作業時、データの交換サーバから電子文書を作業者端末にダウンロードして承認（電子署名の付与）等を行うことも多い。ところが、この場合ダウンロードした電子文書、つまりオフライン下での電子文書自体にはサーバの管理が及ばず、機密性の維持に問題を生ずる可能性が残る。

【０００９】

さらに、上記特許文献等に開示された従来システムでは、電子文書についてサーバ管理下ではセキュリティが確保されているが、複数の項目が設定された所定のフォームが設定されている電子文書において、各項目に入力されているデータを個別に保護することの必要性については全く考慮がない。

【００１０】

複数のユーザの間で電子文書を回覧する場合（途中で文書内容に変更がない場合）や、電子文書の稟議の場合などであれば、アクセス権限のないユーザに対して、電子文書全体の機密性が維持されていればよい。このような場合には、電子文書を暗号化してネットワークを介して送信するという方法でも機密性は維持できる。

【００１１】

しかし、電子文書に設定された複数の項目に対して、各ユーザが、それぞれ、本来は個別に守秘すべきデータを入力して順に電子文書を受け渡す、言い換えると、アクセス権限が、順次、次のユーザに移るようなワークフローの場合には、後に入力するユーザは、先のユーザが入力したデータを全て閲覧することができてしまう。

【００１２】

例えば、特許文献１では、上述のように、該当するユーザの権限に応じて、表示する項目を制御するが、これは作業効率の向上のためであり、データベースに保管される電子文書について項目毎のセキュリティ管理は行われていない。つまり、データベースにアクセスしたユーザが、例えばフルテキスト検索のような検索処理を実行すると、モニタに表示されていないだけの電子文書の他の項目への入力データを閲覧できてしまう可能性がある。または、仮にデータベースから格納されていた電子文書が漏洩した場合、電子文書のいずれの項目についても機密性を維持することはできない。

【００１３】

本発明は、複数項目を有するフォームを備えた電子文書において、個々の項目の機密性を維持しながらのワークフローを実現する。

【課題を解決するための手段】

【００１４】

本発明は、複数の項目を備えるフォームを備える電子文書の処理プログラムであり、この電子文書は、前記複数の項目がそれぞれ別のオブジェクトとして定義され、オブジェクト毎に異なる鍵、又は同一グループとして分類されたオブジェクトのグループ毎に異なる鍵を用いて、各項目に入力されたデータを暗号化して得る暗号化データの格納部と、前記オブジェクト毎又は前記グループ毎に、前記暗号化データを権限あるユーザに対して復号化するための復号化情報を格納する復号化情報の格納部と、を備える。そして、処理プログラムは、コンピュータに、各ユーザに与えられた権限を判定する判定処理、所定のユーザが前記電子文書を開いた際、前記復号化情報に基づいて、該ユーザに閲覧権限が与えられた前記オブジェクト毎又は前記グループ毎に暗号化データを復号化する復号化処理、を実行させる。

【００１５】

本発明の他の態様では、上記処理プログラムにおいて、前記復号化情報は、オブジェクト毎又はグループ毎に、ユーザ識別情報と、ユーザ権限情報とを備え、コンピュータに、該電子文書に格納されている前記ユーザ識別情報及び前記ユーザ権限情報とに基づいて、前記電子文書を開いたユーザに対する権限を判定させ、前記電子文書を開いたユーザが閲覧権限を持たない前記オブジェクト又は前記グループについて、暗号化データが存在する場合、コンピュータモニタに対し、対応する項目には格納されている該暗号化データ又は該暗号化データに代えて任意の判読不能なデータを表示させ、又は項目を非表示とする。前記電子文書を開いたユーザが閲覧権限を持つ場合には、該当する暗号化データを復号化させ、得られた復号化データを対応する項目のデータとして前記コンピュータモニタに表示させる。

【００１６】

本発明の他の態様では、上記電子文書の処理プログラムにおいて、該電子文書の前記各項目における入力データの有無を判定させ、該データの有無に応じて、前記オブジェクト毎又は前記グループ毎のユーザ権限を設定する。また、前記電子文書が各項目における入力データの有無から、該電子文書のステータスを判定するステータス判定部を備える場合には、前記電子文書が開かれる際、コンピュータに、該ステータス判定部での判定を実行させ、判定されたステータスに応じて、前記オブジェクト毎又は前記グループ毎にユーザの権限を設定させる。

【００１７】

本発明の他の態様では、上記電子文書の処理プログラムにおいて、コンピュータに、さらに、前記ユーザが入力権の設定された前記項目に入力したデータを、該データを該当する項目のオブジェクト毎又はグループ毎の鍵によって暗号化する暗号化処理と、前記電子文書の暗号化データの格納部に格納する格納処理と、を実行させる。さらに、ユーザに対して復号化されたデータについても対応する鍵で暗号化してもよい。

【００１８】

本発明の他の態様では、複数の項目を備えるフォームを備える電子文書の処理装置であって、前記電子文書は、前記複数の項目がそれぞれ別のオブジェクトとして定義され、オ

ブジェクト毎に異なる鍵、又は同一グループとして分類されたオブジェクトのグループ毎に異なる鍵を用いて、各項目に入力されたデータを暗号化して得る暗号化データの格納部と、前記オブジェクト毎又は前記グループ毎に、前記暗号化データを権限あるユーザに対して復号化するための復号化情報を格納する復号化情報の格納部と、を備える。処理装置は、各ユーザに与えられた権限を判定するユーザ権限判定手段と、所定のユーザが前記電子文書を開いた際、前記復号化情報に基づいて、該ユーザに閲覧権限が与えられた前記オブジェクト毎又は前記グループ毎に暗号化データを復号化する復号化手段と、を備える。

【発明の効果】

【００１９】

電子文書の各項目を別のオブジェクトとして定義し、項目への入力データを、オブジェクト毎又はオブジェクトが分類されたグループ毎に個別の鍵で暗号化して暗号化データを格納する。そして、その項目について閲覧権限のあるユーザに対してのみ復号化する。つまり、電子文書の項目毎にユーザのアクセス権限、特に項目毎に閲覧権限が制御される。

【００２０】

よって、閲覧権限がないユーザは、電子文書を全文検索するなどしても非復号化データの内容を判読することができず、ワークフローの後にいるユーザに対して項目毎の機密性を維持したまま電子文書を処理させることができる。

【００２１】

電子文書に各項目へのデータ入力状況に応じて文書のステータスを判定するための変数やプログラムを内在させ、処理装置がそのプログラムなどを実行することで、特定のワークフローサーバは必要とせず、文書自体でワークフローを実現できる。例えば最初は全ユーザも文書を開いて初期状態の電子文書の項目を閲覧できるが、最初のユーザが個人情報などの所定のデータを入力し、保存した後は、そのユーザと、このユーザの後にこの電子文書を処理するユーザであって、その項目に対して閲覧権限あるユーザにしか閲覧させないという管理ができる。さらに、最初のユーザでも、次のユーザが入力した後には入力済みのデータを編集できないというような管理も可能であり、承認後の修正などを禁止し承認の信頼性を高めるなども可能である。

【００２２】

さらに、オンラインのポリシー管理サーバと組み合わせて、ユーザ権限などを変更することも可能である。

【発明を実施するための最良の形態】

【００２３】

以下、本発明の実施の形態（以下実施形態という）について、図面を参照して説明する。

【００２４】

［電子文書及び電子文書処理システムの概要］

図１は、本実施形態に係る電子文書の概略構成、図２は、この電子文書の処理システムの概要を示している。

【００２５】

電子文書１０は、１まとまりとして定義された電子ファイルであり、大別すると、最終的に人が理解することのできるデータ部１００（テキストデータ、画像データ、音声データ等であり、これらのデータがバイナリデータとして存在している場合を含む）と、電子文書及びこれを処理するシステムプログラムが用いる制御部２００（フォーム情報、復号化情報、タグ、制御コード、制御プログラム（ステータス判定プログラムなど））、ヘッダ情報等）を備える。なお、図１では、データ部１００と制御部２００を分離して示しているが、もちろん、これは概念的に区別されることを意味しているのであり、実際にデータが分離されている構成には限定されない。

【００２６】

また、本実施形態の電子文書１０は、複数の項目を備えたフォームが設定され、各項目がそれぞれ別のオブジェクトとして定義されている。また、オブジェクト毎、又は同一グ

ループとして分類されたオブジェクトのグループ毎に異なる鍵を用いて、各項目に入力されたデータを暗号化して得る暗号化データの格納部１２０を備える。

【００２７】

さらに、オブジェクト毎又はグループ毎に、権限あるユーザに対して暗号化データを復号化するための復号化情報を格納する復号化情報の格納部２１０を備える。なお、本実施形態では、各オブジェクトがそれぞれ分類されてグループ分けされている。さらに、後述するように、どのグループにも固有のグループ識別情報（グループＩＤ）が付されている。

【００２８】

フォームは、所定の項目が所定の関係で存在し、又は表示されるように決めた形式である。図１の例では、この電子文書は、４つの項目が設けられており、例えば、項目ｉ０は受付番号、項目ｉ１は氏名情報、項目ｉ２は、住所及び電話番号情報、項目ｉ３は、電子文書の承認者名及び電子署名情報と定義されている。つまり、フォーム情報は、項目数、項目とその項目に格納されるべき情報との対応関係を指定している。各ユーザ端末のモニタにおいて、完全に同一の表示レイアウトが実現されなくとも良いし、同一レイアウトが提供されても良い。

【００２９】

各項目を別のオブジェクトとして定義する方法は、電子文書のファイル形式等に応じて様々であるが、項目に対応したデータ領域を、例えばそれぞれ所定のタグで識別したり、制御コード等で識別可能に設定することで実現できる。或いは、電子文書のデータ部１００において、文字データ配列の１行文字数、１頁行数などを指定するフォームを用いる場合には、各項目に対応するデータ位置を、その行位置などを指標に識別することも可能である。

【００３０】

また、各項目の暗号化データ格納部１２０は、１ファイル内に連続配置され、間がタグなどで区切られて配列されていても良し、ランダムに配置され、特定のインデックスから参照される形式でもよい。

【００３１】

このように本実施形態では、電子文書１０それ自体が、フォーム情報、また、復号化情報、及び既に入力されている場合には暗号化データを備える。したがって、この電子文書を処理するシステムにワークフローを管理するサーバは不要であり、システムの最小単位は、図２に示すように、この電子文書を処理する機能を備えた電子文書プログラム４００を持つコンピュータ、つまり、各ユーザが用いる端末（ユーザ端末又はクライント端末）３０である。

【００３２】

ユーザ端末３０は、各処理を実行するためのＣＰＵ３１０、所定ファイル、プログラムなどを保存する蓄積装置３２０、ユーザが本システムを操作するためのキーボード・マウスなどの入力装置３３０、本システムからユーザへの情報を表示するモニタなどの表示装置３４０、プログラム、システムデータ、通信情報等を記憶するメモリ部３５０、認証、ファイル保存、メール送受信などを行うサーバ５００との間でネットワークを介して、データのやり取りを行うためのネットワーク制御部３６０等を備える。

【００３３】

なお、本実施形態において、端末３０は、従来のように電子文書を保管し、またユーザ権限、ワークフローを管理する管理サーバ（ポリシー管理サーバ）に接続されない状態（オフライン）でも、上記電子文書１０の取り扱いが可能であるが、もちろん、後述するようにポリシー管理サーバ５００の管理下（オンライン）でもその取り扱いを実行可能としても良い。

【００３４】

電子文書プログラム４００は、上述の電子文書１０を取り扱うプログラムであり、いわゆるアプリケーションソフトウエア等によって構成される。このプログラム４００は、よ

り具体的には後述するが、コンピュータ３００に、電子文書の項目データを暗号化を実行させるモジュール、電子文書内の復号化情報を用いて復号化を実行させるモジュール、ユーザ認証のための処理（パスワード処理、パブリックキー処理）のためのモジュール、ステータス判定処理を実行させるためのモジュールなどを備える。

【００３５】

［ワークフロー］

次に、本実施形態のシステムにおける電子文書の処理フロー（ワークフロー）について、さらに、図３及び図４を参照して説明する。図３は本実施形態の電子文書のワークフロー、図４は、図３のワークフローの各段階でユーザに提供される電子文書の状態を概念的に示している。

【００３６】

ここで、上記の通り本実施形態の電子文書処理フローはオフラインで実行できるため、まず、オフライン状態（ポリシー管理サーバによる管理がない状態）でのフローを説明する。

【００３７】

電子文書１０の各項目に対する権限は、各ユーザに設定されたアクセス権限に応じ、入力可能か不可能か、そして、入力データの判読可能（可視）か、判読不能（不可視）かについて設定されている。この判読不能状態は、単なる非表示ではなく、暗号化された入力データが存在する場合でも復号化しないことを意味し、暗号化データをそのまま表示する方法（内容の判読不能）と、暗号化データに代えて＊＊＊等の伏字で表示する方法（内容の判読不能）、そして、もちろん非表示（すなわち空欄として表示）とする方法等が採用可能である。図４の例では、伏字で表示する方法を採用した場合の例である。なお、機密性の維持の問題がない項目については、ユーザの入力・承認などの作業効率向上等の観点で、復号化された入力データを単に画面上に非表示とする設定を行っても良い。

【００３８】

各項目に対して設定される権限は、上記のように入力許可と判読許可に大別できるが、図４の例では、その組み合わせにより４通り設定されている。ｉＳ１で示す項目権限は、項目の存在及び入力データは判読でき（可視）、かつ、データの入力が可能である。ｉＳ２で示す項目権限は、項目の存在及び入力データが存在する場合はそのデータが判読できるが、データの入力は禁止されている（入力不可）。ｉＳ３で示す項目権限は、項目の存在又は項目の内容が判読できず（不可視）、入力もできない（入力不可）。ｉＳ４で示す項目状態は、項目の存在（及び種類）は判読できるが、入力データが存在している場合（暗号化データ）、そのデータは復号化されずに暗号化データに代えた伏字で表示され（判読不能）、また、入力もできない（入力不可）。

【００３９】

電子文書を取り扱う権限のあるユーザとしては、ここでは、図３に示すようにＡ，Ｂ，Ｃの３名が設定され、ユーザＡは電子文書の所定項目への初期入力者、ユーザＢは受付担当者、ユーザＣは、最終処理者である。

【００４０】

まず、初期入力者であるユーザＡには、どの項目にもデータの入力されていない初期状態の電子文書１０が提供され、ユーザＡが端末から開封指示をすると、ユーザＡの端末のモニタには図４（ａ）のような画面が表示される。ユーザＡには、項目ｉ１、ｉ２（ここでは、氏名の項目と、住所及び電話番号の項目）にのみデータ入力権限が与えられており、これらの項目は、状態ｉＳ１（可視、入力可）になる。項目ｉ０（受付番号）は、項目の存在及び存在する場合、内容を見ることができるが入力はできない状態に制御される（状態ｉＳ２）。なお、項目ｉ３（承認者、電子署名）は、状態ｉＳ３（不可視、入力不可）の状態となり、図４（ａ）の例では、項目名自体も全く表示されていない。ユーザＡが、データ入力を終え、電子文書の保存指示を行うと、入力されたデータは、項目ｉ１，ｉ２にそれぞれに割り当てられた暗号鍵で暗号化され、図１に示す電子文書１０の暗号化データ格納部１２０に得られた暗号化データが格納される。

【００４１】
保存された電子文書１０は、ユーザＡから次にユーザＢに渡される。電子文書１０の受け渡しは、どのような手段でも良く、例えばネットワークを通じた電子メール送信などによって行うことができる。
【００４２】
ユーザＢは、ユーザＡが入力した電子文書１０を受け取り、この電子文書１０を開封し、ユーザＢに入力権限の与えられた項目にデータを入力する。図４（ｂ）の例で、ユーザＢに入力権限のある項目は、ユーザＡに入力権限が与えられた項目ｉ１，ｉ２とは異なり、項目ｉ０（受付番号）である。また、ユーザＢは、ユーザＡがデータ入力した項目ｉ１，ｉ２の内、一部はその入力データの判読が可能（閲覧可能）で、一部は判読不能に権限設定されている。図４（ｂ）の例では、項目ｉ１（氏名）については暗号化された入力データが復号化されていて判読可能であるが、項目ｉ２（住所及び電話番号）は、伏字「＊」で表示されていて、データが存在することが認識できるが、内容については判読不能となっている。なお、項目ｉ３（承認者及び電子署名）については、入力不可であるが判読可能となっている。ユーザＢがデータ入力後、電子文書の保存指示を行うと、入力されたデータは、この項目（受付番号の項目）に割り当てられた暗号鍵で暗号化される。さらに、ユーザＢに対し、復号化により判読可能に表示されたユーザＡによる入力データについても、この項目に個別の鍵で暗号化され、それぞれ、図１に示す電子文書１０の暗号化データ格納部１２０に格納される。項目ｉ３については、記入がなく、このようにデータの存在しない項目については、暗号化処理はしなくても良い。以上のように、ユーザＡよりも後に処理するユーザＢに対し、既に先のユーザＡによってデータ入力されている項目であっても機密性を維持したまま、ユーザＢに入力業務を実行させ、次のユーザに電子文書を受け渡すことが可能となっている。
【００４３】
ユーザＢが保存した電子文書１０は、次に、ユーザＢからユーザＣに渡される。この電子文書１０の受け渡しも、どのような手段でも良く、例えばネットワークを通じた電子メール送信などによって行うことができる。
【００４４】
ユーザＣには、電子文書１０のフォームで設定された項目ｉ０～ｉ２に対し、ユーザＡ及びＢによる入力データについての承認権限が与えられており、ユーザＡ及びＢがそれぞれ入力したいずれの項目についても、その入力データの判読可能（閲覧可能）となっている。よって、ユーザＣは、項目ｉ０（受付番号）、項目ｉ１（氏名）、項目ｉ２（住所及び電話番号）にそれぞれ判読可能に表示されたデータについて誤りがないかどうか確認し、或いは入力されていることを確認し、項目ｉ３に承認者名を入力し、自分の電子署名を付す。この電子署名は、例えば承認後に改竄がないことを証明するためのものであり、公開鍵暗号方式を利用した証明性の高いいわゆるデジタル署名とすることができる。
【００４５】
本実施形態の電子文書処理システムは、上記のようにオフラインにおいて各項目のデータの機密性を維持しながら電子文書を処理することができるが、図５に示すように、ポリシー管理サーバ６００の管理下、即ち、オンラインでも処理をすることが可能である。ポリシー管理サーバ６００は、電子文書のフォームの各項目に対するユーザ毎のアクセス権限を管理する。また、ユーザ認証サーバ６１０は、電子文書にアクセスする権限を判定する際のユーザ認証を実行する。
【００４６】
本実施形態において、ポリシー管理サーバ６００は、電子文書内に添付される復号化情報（ユーザ識別情報や、ユーザ権限情報など書き換え権限、下記ステータス判定結果や、判定プログラムの修正などについても管理し、また変更する機能を持たせることができる。電子文書自体は、オフラインの場合と同様に、ユーザ間で受け渡され、ユーザＡが入力したデータ及びユーザＡが閲覧しデータは、ユーザＡが電子文書を保存する際に暗号化されて、次のユーザＢに渡される。

【００４７】
ここで、例えばユーザが電子文書を開く操作をした際に、電子文書処理プログラム４００が、ポリシー管理サーバ６００にアクセス可能かどうかを判定し、アクセス可能な場合には、そのユーザのユーザ識別情報やパスワードその他の認証情報、及びその電子文書の識別情報をポリシー管理サーバ６００に送る。ポリシー管理サーバ６００は、その情報を基にユーザ認証を行い、そのユーザに対して付与されたその電子文書の各項目についてのアクセス権限の情報、言い換えれば復号化情報、を自身のデータベースから読み出して、ユーザ側の電子文書処理プログラム４００に返す。これを受け取った電子文書処理プログラム４００は、受け取った復号化情報により当該電子文書内の復号化情報を更新した上で、上述と同様の処理を行う。

【００４８】
このようにポリシー管理サーバ６００の管理下でもワークフローを実行可能とすることで、電子文書への入力状態等にかかわらずに権限を変更でき、ワークフローの変更要求に即座に対応することができる。

【００４９】
［ステータス判定］
次に、電子文書のステータス判定について説明する。オフライン状態で機密性を維持しつつ電子文書を受け渡す必要があるため、電子文書への各項目への入力状況を判断して最適なアクセス権限を設定する機能を備えることが好適である。つまり、入力データの有無によってもセキュリティレベルを変更するのである。これは、一例を挙げれば、上記ワークフローにおいて、ユーザＡは、初期状態の電子文書に対して項目ｉ１，ｉ２の入力権限（編集権限）を有するが、仮に、ユーザＢが項目ｉ０にデータを入力した後、ユーザＡが再び電子文書を開いても、入力済みの項目ｉ１、ｉ２は、閲覧できるが、再編集することができないように権限が変更されるというようなことである。

【００５０】
この電子文書のステータス判定は、電子文書を開き、暗号化データが存在する場合にそれを復号化する前に実行する必要がある。ステータスは文書中に変数として定義され、この変数をユーザ端末３０の電子文書処理プログラムが解析しステータスを判定することができる。または、電子文書中にステータス判定を実行するためのプログラム（モジュール）を内包させ、このプログラムを電子文書をユーザが開く際に実行させることによりステータス判定を実行してもよい。

【００５１】
図６は、電子文書の各項目に定義された変数の例、図７は、ここではＪＡＶＡＳＣＲＩＰＴ（登録商標）で作られたステータス判定プログラムの一例を示す。

【００５２】
フォームの各項目に定義された変数は、ここでは、図６に示すように「Ｄｏｃ．ｆｏｒｍ［　］．「ｅｌｅｍｅｎｔｓ［　］」で表現されているが、もちろんこのような表現には限定されない。項目ｉ２（住所、電話番号）を例に説明すると、住所項目は、「Ｄｏｃ．ｆｏｒｍ［ｉ２］．ｅｌｅｍｅｎｔｓ［１］」、電話番号は、「Ｄｏｃ．ｆｏｒｍ［ｉ２］．ｅｌｅｍｅｎｔｓ［２］」と定義されている。図２の電子文書プログラム４００や、図７に示す下記電子文書内のステータス判定プログラムは、この変数に対し、データが入力されているかどうかを判定する。

【００５３】
図７の例では、いずれの項目にもデータが入力されていない場合、ステータス（temp）は、０と判定される。項目ｉ１の氏名項目にデータが入力され、項目ｉ２の住所欄、電話番号にそれぞれデータが入力されている場合、ステータスは１と判定される。ステータス１の条件に加え、さらに項目ｉ０の受付番号が入力されている場合、ステータスは２、さらに項目ｉ３の承認者、電子署名にデータ入力があれば、ステータスは３と判定する。よって、例えば、図６のように、項目ｉ０、ｉ１、ｉ２にデータが入力済みであれば、ステータスは「２」と判定し、ステータスに応じて予め各ユーザに対して決められたユーザ権

限を適用する（下表参照）。

【００５４】

なお、図７のプログラム例において、項目への入力データの正当性は、データ入力時または電子文書保存時に確かめられると仮定して、入力されているかどうかのみを確認している。項目への入力データの正当性は、これを評価する場合どのような方法でも良く、例えば、各ユーザが電子文書保存時にその時点の全項目や入力項目に対してデジタル署名を施すなどの方法を採用することができる。

【００５５】

ここで、図７に示されるようなステータス判定プログラム（スクリプト）は、暗号化して電子文書に添付しても良いが、暗号化せず、その代わり改竄されていないかどうかを電子署名等の適切な手段を採用することで、検知することが可能である。いずれの場合にも電子文書のステータス判定は、オフライン状況で、電子文書とこれを処理するユーザ端末によって、電子文書のワークフロー上での位置を検出して最適なアクセス権限に設定していく上で重要であり、改竄されないように対策しておくことが好適である。

【００５６】

［オブジェクトの分類］

本実施形態の電子文書は、上記のように各項目を別のオブジェクトとして定義し、オブジェクトはそれぞれ所定グループに分類され、所属するグループのグループＩＤ（暗号化グループＩＤ）が付されている。１グループのオブジェクト数は１以上で、グループは、項目内容、ユーザ権限、ワークフローの態様（順番）などに応じて決める。全ての項目について異なる暗号化の鍵を用いて入力データを暗号化しても良いが、グループ分けし、グループ毎に付した暗号化グループＩＤを利用した鍵を使うことにより、暗号化、復号化を効率的に実行することが可能となる。

【００５７】

暗号化グループＩＤは、図８のように、各オブジェクト領域内に対応する暗号化データ（Ｘα、Ｘβ、Ｘγ）と関連づけて付与しておくことができる。また、図９のように、電子文書内に暗号化グループＩＤと、このグループに属するオブジェクトとの参照テーブルを持ち、各オブジェクトの暗号化グループＩＤをこの参照テーブルを用いて管理してもよい。復号化を実行する際、あるいは暗号化する際、この参照テーブルを参照することで、処理対象となる項目に対応する暗号化グループＩＤを特定することができる。

【００５８】

図８のようにオブジェクト毎に暗号化グループＩＤを付与する場合、一般的に、各オブジェクトを前から順に処理していくので、参照テーブル等にアクセスして解析するなどの作業が不要であるため、上記暗号化、復号化の処理をより迅速に実行することが容易である。図９のように参照テーブルを利用する場合には、グループに属するオブジェクトの変更等の際、参照テーブルを修正するだけで良く、修正が容易である。またこの参照テーブルを用いれば、同一暗号化グループＩＤが付されたオブジェクトを特定できるため、例えば復号化の際の復号すべき項目の判断等が容易である。

【００５９】

なお、図７のプログラム例において、項目への入力データの正当性は、データ入力時または電子文書保存時に確かめられると仮定して、入力されているかどうかのみを確認している。項目への入力データの正当性は、これを評価する場合どのような方法でも良く、例えば、各ユーザが電子文書保存時にその時点の全項目や入力項目に対してデジタル署名を施すなどの方法を採用することができる。この場合、ユーザは、直前のユーザから受け取った電子文書に付された電子署名をその直前ユーザの公開鍵証明書を用いて検証することで、改竄の有無を確認できる。

【００６０】

ここで、図７に示されるようなステータス判定プログラム（スクリプト）は、暗号化して電子文書に添付しても良いが、暗号化せず、その代わり改竄されていないかどうかを電子署名等の適切な手段を採用することで、検知することが可能である。いずれの場合にも

電子文書のステータス判定は、オフライン状況で、電子文書とこれを処理するユーザ端末によって、電子文書のワークフロー上での位置を検出して最適なアクセス権限に設定していく上で重要であり、改竄されないように対策しておくことが好適である。

【００６１】

【表１】

ステータス１

	ユーザ１	ユーザグループ２
暗号化ＧＩＤ　α	編集可能	編集不可、可視
暗号化ＧＩＤ　β	編集不可、不可視	編集不可、可視

ステータス２

	ユーザ１	ユーザグループ２
暗号化ＧＩＤ　α	編集不可、可視	編集可能
暗号化ＧＩＤ　β	編集不可、不可視	編集可能

【００６２】

［暗号化処理］

次に、本実施形態に係る暗号化処理について説明する。項目に入力されているデータについての暗号化は、電子文書を開いたユーザがこの電子文書を保存する際に、実行される。但し、より高い機密性を実現する場合には、データ入力後（データ確定後）、直ちに暗号化を実行しても良い。

【００６３】

暗号化の対象は、この電子文書を開いたユーザが入力したデータ、又はこのユーザに対して復号化されて判読可能となったデータの両方のデータである。

【００６４】

上述のように、各オブジェクトのデータの暗号化の鍵は、このオブジェクトが属するグループに付された暗号化グループＩＤ毎に割り当てられる鍵である。暗号化のアルゴリズムに関しては用途に見合った適当なものを用いればよいが、各グループごとに異なる暗号鍵を用いることが必要である。

【００６５】

［復号化情報］

復号化情報について図１０をさらに参照して説明する。図１の各電子文書１０にはその復号化情報格納部２１０に、復号化のための情報（復号化情報）Ｘα、Ｘβが格納されている。この復号化情報Ｘは、暗号化グループＩＤ毎に、例えば配列として定義されおり、一例として以下のような情報を含む。

（１）ユーザを識別する識別情報（ユーザＩＤ）

（２）ユーザＩＤの正当性をチェックするための情報（例えば、パスワードやＰＫＩのサーバなど）

（３）復号化のための鍵を生成する情報

（４）各グループ（暗号化グループＩＤ）に対するユーザ権限

本実施形態において、例えば、ＰＫＩ（公開鍵暗号基盤）に基づいて、暗号化、認証、デジタル署名等を実行する場合において、このＰＫＩで用いられるＰｕｂｌｉｃ　Ｋｅｙ　Ｃｒｙｐｔｏｇｒａｐｈｉｃ　Ｓｔａｎｄａｒｄ　＃７　Ｂｉｎａｒｙ　Ｅｎｃｏｄ

ｉｎｇ　Ｓｙｎｔａｘでは権限の違いごとのバイナリデータになっており、そのバイナリデータには、同じ権限を有するユーザのユーザＩＤ群と復号化のための鍵を生成するための情報が入っている。よって、この場合、このバイナリデータを復号化情報として暗号化グループＩＤ毎に上記復号化情報格納部２１０に格納しておく。

【００６６】

［電子文書の開封時処理］

次に、図１１を参照して、電子文書の開封時の処理について説明する。

【００６７】

ユーザが電子文書処理装置の入力手段を用い、電子文書に対する開封要求を行うと、処理装置は、電子文書が改竄されていないかどうかを確認する（Ｓ１）。改竄の確認は、少なくとも、電子文書内にステータス判定プログラムを備える場合にこのプログラムに改竄が無いかどうかの確認である。もちろん、各ユーザに受け渡されるまでの間に電子文書が改竄されていないかどうかを電子署名等を利用して実行してもよい。

【００６８】

改竄の判断ステップ（Ｓ２）で、改竄があると判断された場合（Ｙｅｓ）には、エラー処理とし、電子文書の開封は実行しない（Ｓ３）。

【００６９】

改竄が無いと判断された場合（Ｎｏ）、開封要求された電子文書のステータスの判定が行われる（Ｓ４）。ステータスの判定は、上述のように電子文書処理プログラムまたは電子文書中の判定プログラムを用い、電子文書の各項目におけるデータの有無に基づいて実行される。

【００７０】

次に、開封要求をしたユーザに対するユーザ認証を行う（Ｓ５）。ユーザ認証は、パスワード認証、ＰＫＩ認証、生体認証など、開封要求したユーザが予め登録された本人であるかどうかを判定し、システムのセキュリティを確保できる手段であれば、特に限定されない。

【００７１】

ユーザ認証が実行されると、ユーザを識別するためのＩＤ（ユーザＩＤ）が特定され、このユーザのオブジェクトへの権限を確認する（Ｓ６）。この権限の確認に際しては、例えば、まず、ステータス判定結果と、復号化情報を参照し、判定された文書ステータスで、復号すべきグループの暗号化グループＩＤを特定する。暗号化グループＩＤの特定に際しては、上述の図８又は図９のような暗号化グループＩＤとオブジェクトとの対応関係を利用することができる。暗号化グループＩＤが特定されると、このＩＤに対応付けられた復号化情報に、処理対象のオブジェクトに対する復号化権限（閲覧権限）があるかどうか確認する（Ｓ７）。

【００７２】

オブジェクトに対する閲覧権限がある場合（Ｙｅｓ）、復号化情報に含まれる鍵生成のための情報から必要な鍵が作成され、オブジェクトが復号化される（Ｓ８）。そして、復号化されたデータのモニターへ表示などの処理が実行される（Ｓ９）。オブジェクトに対する閲覧権限がない場合（Ｎｏ）、他に与えられた権限に応じて、伏字での表示や、項目全体の非表示などの処理が実行される（Ｓ９）。

【００７３】

以上のように権限に応じた表示などの処理が実行され、開封処理は終了する（Ｓ１０）。モニター画面には、図４に例示したように権限に応じた電子文書が表示され、ユーザは、入力、判読、承認、あるいは必要ならば印刷等の処理を実行し、処理後、電子文書の保存を指示すると、上述のように入力データ及び復号化データが、暗号化グループＩＤ毎の鍵により暗号化され、得られた暗号化データは電子文書１０のデータ格納部１２０に保存される。

【００７４】

なお、以上において、項目はｉ０～ｉ３、ユーザはＡ，Ｂ，Ｃの場合を例に挙げている

。しかし、もちろんフォーム及び項目数は図１等の例示には限られず、また、権限設定の組み合わせ、ステータスレベルなど、電子文書のワークフローに応じて様々設定することができる。ユーザ数についても３名に限られずさらに多数でも良いし、フローの順番もＡ，Ｂ，Ｃには限定されず、各段階のユーザがそれぞれ多数設定されていても良い。例えば、初期入力者Ａが、Ａ１，Ａ２，Ａ３・・Ａｎと多数設定されるなども可能である。

【図面の簡単な説明】

【００７５】

【図１】本実施形態に係る電子文書を概念的に説明する図である。

【図２】本実施形態に係る電子文書処理システムを概念的に説明する図である。

【図３】本実施形態に係る電子文書の処理フローを説明する図である。

【図４】図３のフローをモニターへの電子文書の表示例で説明する図である。

【図５】ポリシー管理サーバによる管理下での電子文書の処理フローを説明する図である。

【図６】ステータスを判定するために定義された変数を説明するための図である。

【図７】ステータス判定プログラムの一例を示す図である。

【図８】オブジェクト毎に暗号化グループＩＤを付す方法を概念的に示す図である。

【図９】オブジェクトの暗号化グループＩＤ毎の参照テーブルを説明する図である。

【図１０】オブジェクトの復号化のための情報の格納方法を概念的に示す図である。

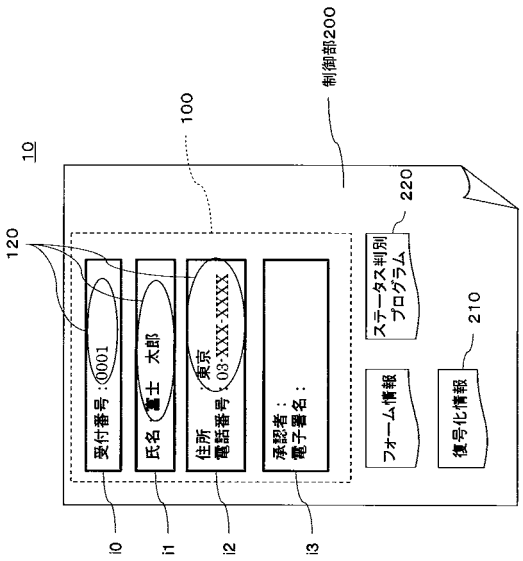
【図１１】本実施形態に係る電子文書の開封時の処理フローを示す図である。

【符号の説明】

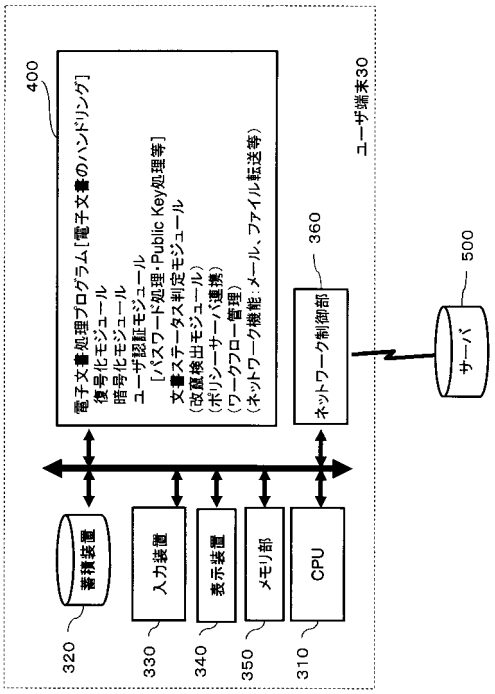
【００７６】

１０　電子文書、３０　ユーザ端末、１００　データ部、１２０　暗号化データ格納部、２００　制御部、２１０　復号化情報格納部、２２０　ステータス判定プログラム、４００　電子文書処理プログラム。

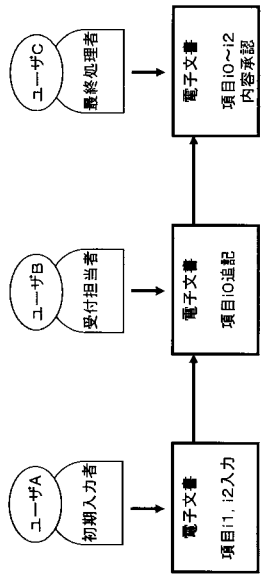
【図１】



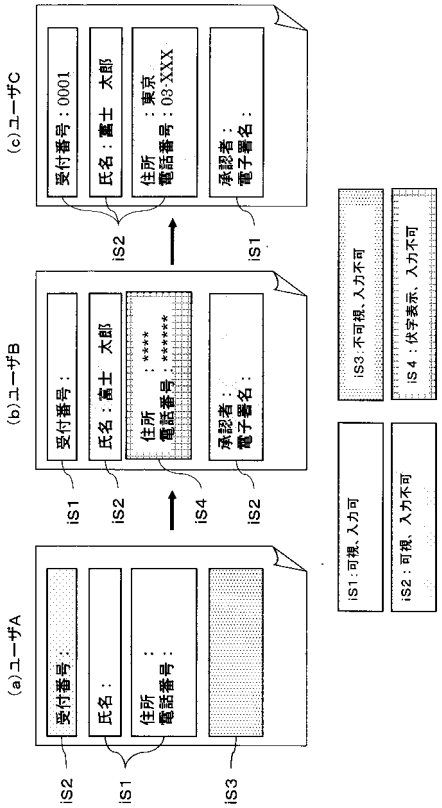
【図２】



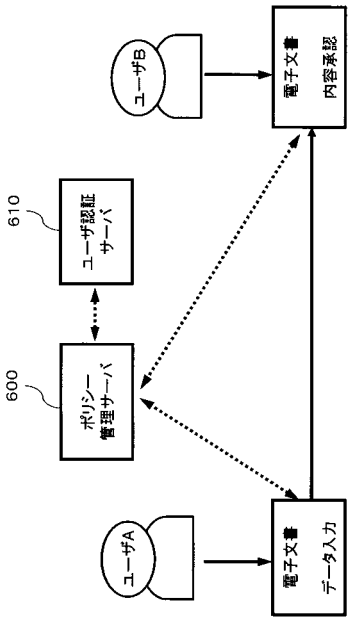
【図３】


ユーザA
初期入力者
電子文書
項目i1, i2入力
ユーザB
受付担当者
電子文書
項目i0追記
ユーザC
最終処理者
電子文書
項目i0~i2
内容承認

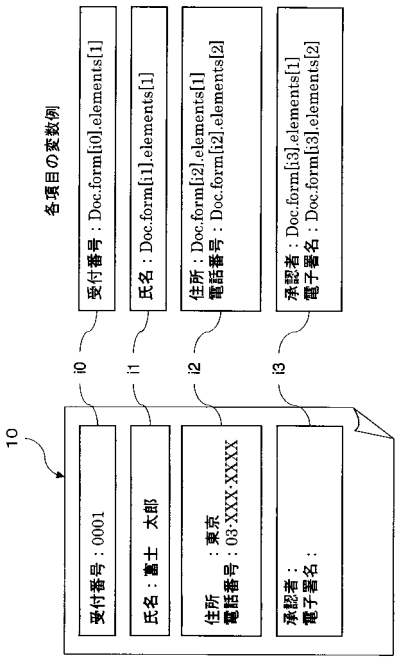
【図４】


(a)ユーザA
受付番号：
氏名：
住所 ：
電話番号：
(b)ユーザB
受付番号：
氏名：富士 太郎
住所 ：****
電話番号：******
承認者：
電子署名：
(c)ユーザC
受付番号：0001
氏名：富士 太郎
住所 ：東京
電話番号：03-XXX
承認者：
電子署名：
iS1
iS2
iS3
iS4
iS1：可視、入力可
iS2：可視、入力不可
iS3：不可視、入力不可
iS4：伏字表示、入力不可

【図５】


ユーザA
ユーザB
電子文書
データ入力
電子文書
内容承認
ポリシー
管理サーバ
600
ユーザ認証
サーバ
610

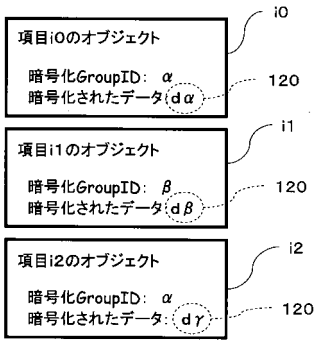
【図６】


各項目の変数例
受付番号：Doc.form[i0].elements[1]
氏名：Doc.form[i1].elements[1]
住所：Doc.form[i2].elements[1]
電話番号：Doc.form[i2].elements[2]
承認者：Doc.form[i3].elements[1]
電子署名：Doc.form[i3].elements[2]
i0
i1
i2
i3
10
受付番号：0001
氏名：富士 太郎
住所 ：東京
電話番号：03-XXX-XXXX
承認者：
電子署名：

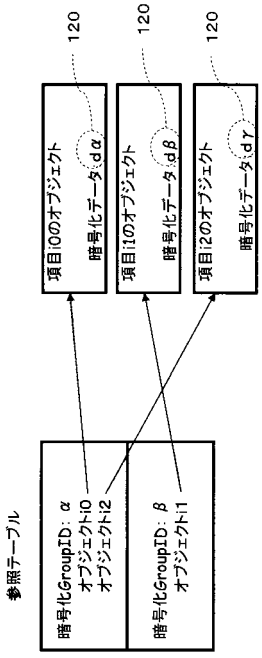
【図７】

```
function checkDocumentStatus(status) {

        temp = 0;       //何も入力されていない状態0

        if ((Doc.form[1].elements[1] != null)
            && (Doc.form[2].elements[1] != null)
            && (Doc.form[2].elements[2] != null)) {
          temp = 1;       /氏名、住所、電話番号が入力された状態1
        }

        if ((temp == 1)
            && (Doc.form[0].elements[1] != null)) {
          temp = 2;       //状態1に加え、受付番号が入力された状態2
        }

        if ((temp == 2)
            && (Doc.form[3].elements[1] != null)
            && (Doc.form[3].elements[2] != null)) {
          temp = 3;       //状態2に加え、承認者と電子署名が入力された状態3
        }

        status = temp

}
```

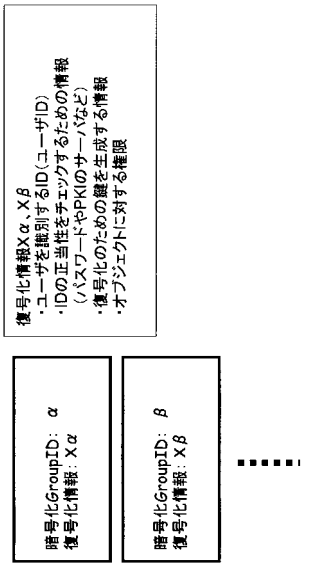
【図８】



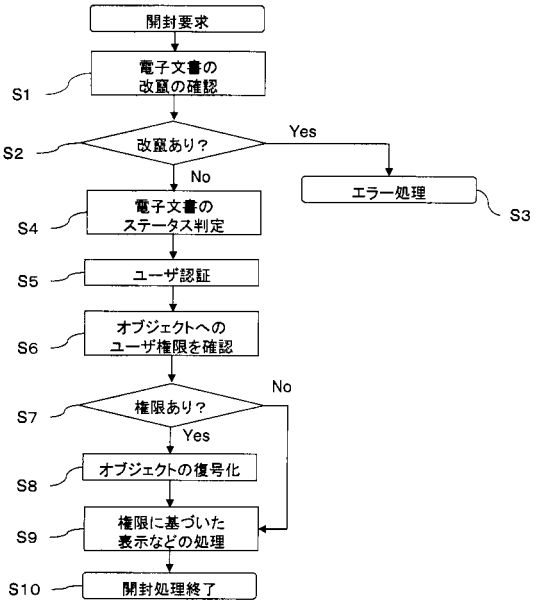
【図９】



【図１０】



【図１１】


開封要求
電子文書の
改竄の確認
S1
改竄あり？
S2
Yes
No
エラー処理
S3
電子文書の
ステータス判定
S4
ユーザ認証
S5
オブジェクトへの
ユーザ権限を確認
S6
権限あり？
S7
No
Yes
オブジェクトの復号化
S8
権限に基づいた
表示などの処理
S9
開封処理終了
S10

フロントページの続き

(51)Int.Cl.	FI			テーマコード（参考）
	Ｇ０６Ｆ	12/14	５３０Ｅ	
	Ｇ０６Ｆ	12/14	５６０Ｃ	
	Ｇ０６Ｆ	12/14	５６０Ｂ	