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

特許第4664572号
(P4664572)

(45)発行日　平成23年4月6日(2011.4.6)　(24)登録日　平成23年1月14日(2011.1.14)

(51)Int.Cl.		F I		
G06F 17/21	(2006.01)	G06F	17/21	570M
G06F 21/24	(2006.01)	G06F	17/21	570R
		G06F	12/14	520P
		G06F	12/14	550Z
		G06F	12/14	560C

請求項の数 3　(全 50 頁)

(21)出願番号　特願2002-205669(P2002-205669)
(22)出願日　平成14年7月15日(2002.7.15)
(65)公開番号　特開2003-228560(P2003-228560A)
(43)公開日　平成15年8月15日(2003.8.15)
審査請求日　平成16年10月4日(2004.10.4)
審判番号　不服2008-46(P2008-46/J1)
審判請求日　平成20年1月4日(2008.1.4)
(31)優先権主張番号　特願2001-361470(P2001-361470)
(32)優先日　平成13年11月27日(2001.11.27)
(33)優先権主張国　日本国(JP)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　110000165
グローバル・アイピー東京特許業務法人
(72)発明者　平野　秀幸
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　橋本　晋二
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54)【発明の名称】文書配布方法および文書管理方法

(57)【特許請求の範囲】
【請求項１】
テキストデータ、画像データ、音楽データ、その他の電子化データで構成される文書データの利用を許可あるいは制限するために必要となる利用制御情報を相補的に構成する第１利用制御情報と第２利用制御情報とを生成し、前記文書データに対して複数の情報項目毎に識別子を設定し、前記識別子内に前記情報項目毎の内容情報を格納するとともに、前記文書データに含まれる管理情報格納用データ内に前記第１利用制御情報を不可視透かしデータとして埋め込み、前記第１利用制御情報が埋め込まれる際の透かし制御情報または透かし制御情報を入手する手段に関する情報である前記第２利用制御情報を前記文書データに含まれる管理用識別子内に埋め込んだ構造化文書のデータ利用装置であって、
配布される文書データの文書構造を解析する文書構造解析手段と、
前記文書データに含まれる管理情報格納用データ内の第１利用制御情報を抽出する手段と、
前記文書データに含まれる管理用識別子内の第２利用制御情報を抽出する第２利用制御情報抽出手段と、
前記第２利用制御情報と、前記文書データに含まれる管理情報格納用データ内の第１利用制御情報とに基づいて、前記文書データの利用を許可あるいは制限する文書データ利用手段と、
を備える文書データ利用装置。
【請求項２】

テキストデータ、画像データ、音楽データ、その他の電子化データで構成される文書データの利用を許可あるいは制限するために必要となる利用制御情報を相補的に構成する第１利用制御情報と第２利用制御情報とを生成し、前記文書データに対して複数の情報項目毎に識別子を設定し、前記識別子内に前記情報項目毎の内容情報を格納するとともに、前記文書データに含まれる管理情報格納用データ内に複数のデータをカプセル化して不可視透かしデータとして前記第１利用制御情報を埋め込み、前記カプセル化されたデータを取り出すための制御情報である前記第２利用制御情報を前記文書データに含まれる管理用識別子内に埋め込んだ構造化文書のデータ利用装置であって、

配布される文書データの文書構造を解析する文書構造解析手段と、

前記文書データに含まれる管理情報格納用データ内の第１利用制御情報を抽出する手段と、

前記文書データに含まれる管理用識別子内の第２利用制御情報を抽出する第２利用制御情報抽出手段と、

前記第２利用制御情報と、前記文書データに含まれる管理情報格納用データ内の第１利用制御情報とに基づいて、前記文書データの利用を許可あるいは制限する文書データ利用手段と、

を備える文書データ利用装置。

【請求項３】

テキストデータ、画像データ、音楽データ、その他の電子化データで構成される文書データの利用を許可あるいは制限するために必要となる利用制御情報を相補的に構成する第１利用制御情報と第２利用制御情報とを生成し、前記文書データに対して複数の情報項目毎に識別子を設定し、前記識別子内に前記情報項目毎の内容情報を格納するとともに、前記文書データに含まれる管理情報格納用データ内に前記文書データの一部を切り取ったものである前記第１利用制御情報を埋め込み、前記文書データ中の第１利用制御情報の位置情報である前記第２利用制御情報を前記文書データに含まれる管理用識別子内に埋め込んだ構造化文書のデータ利用装置であって、

配布される文書データの文書構造を解析する文書構造解析手段と、

前記文書データに含まれる管理情報格納用データ内の第１利用制御情報を抽出する手段と、

前記文書データに含まれる管理用識別子内の第２利用制御情報を抽出する第２利用制御情報抽出手段と、

前記第２利用制御情報と、前記文書データに含まれる管理情報格納用データ内の第１利用制御情報とに基づいて、前記文書データの利用を許可あるいは制限する文書データ利用手段と、

を備える文書データ利用装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、画像データや音楽データなどを含む文書データの配布方法、文書データ生成装置、文書データ利用装置、そのプログラムおよび文書管理方法、文書管理装置、そのプログラムに関する。

【０００２】

【従来の技術】

画像データや音楽データなどの電子化データを含む文書データの真正性を認証可能とする技術として電子署名と呼ばれる技術が知られている。

たとえば、電子化データのハッシュ値を算出し秘密鍵を用いて暗号化した電子署名を電子化データに添付して配布する。配布された電子化データを受け取った利用者は、公開鍵暗号を用いて電子署名を復号化するとともに、電子化データのハッシュ値を算出して、これらが一致するか否かを検証することで、受け取った電子化データの認証を行うことが可能となる。

【０００３】
これにより、配布される文書データに改竄があった場合にこれを検出することができ、不正なデータ配布を防止することができる。
【０００４】
【発明が解決しようとする課題】
しかしながら、電子署名として添付される暗号化データは、可視的なものであり、複数のデータのアルゴリズム解析を行うことで、判読可能になるおそれがある。
また、文書データを構成する画像データに暗号鍵などを不可視の電子透かしとして埋め込むことも提案されているが、この電子透かしを文書データから引き出して利用制御するために、特定のアプリケーションを備えた装置が必要となる。
【０００５】
本発明では、電子化データ内に電子透かしとして埋め込まれた不可視データと、構造化文書内に記述された可視的データとに分離された利用制御情報を用いることにより、文書データの秘匿・隠蔽化、改竄防止、真正性の認証および不正利用防止機能を併せ持つ文書配布方法を提案する。
【０００６】
【課題を解決するための手段】
本発明に係る文書データ利用装置は、テキストデータ、画像データ、音楽データ、その他の電子化データで構成される文書データの利用を許可あるいは制限するために必要となる利用制御情報を相補的に構成する第１利用制御情報と第２利用制御情報とを生成し、文書データに対して複数の情報項目毎に識別子を設定し、識別子内に情報項目毎の内容情報を格納するとともに、文書データに含まれる管理情報格納用データ内に第１利用制御情報を不可視透かしデータとして埋め込み、第１利用制御情報が埋め込まれる際の透かし制御情報または透かし制御情報を入手する手段に関する情報である第２利用制御情報を文書データに含まれる管理用識別子内に埋め込んだ構造化文書のデータ利用装置であって、配布される文書データの文書構造を解析する文書構造解析手段と、文書データに含まれる管理情報格納用データ内の第１利用制御情報を抽出する手段と、文書データに含まれる管理用識別子内の第２利用制御情報を抽出する第２利用制御情報抽出手段と、第２利用制御情報と、文書データに含まれる管理情報格納用データ内の第１利用制御情報とに基づいて、文書データの利用を許可あるいは制限する文書データ利用手段とを備える。
【０００７】
また、本発明に係る文書データ利用装置は、テキストデータ、画像データ、音楽データ、その他の電子化データで構成される文書データの利用を許可あるいは制限するために必要となる利用制御情報を相補的に構成する第１利用制御情報と第２利用制御情報とを生成し、文書データに対して複数の情報項目毎に識別子を設定し、識別子内に情報項目毎の内容情報を格納するとともに、文書データに含まれる管理情報格納用データ内に複数のデータをカプセル化して不可視透かしデータとした第１利用制御情報を埋め込み、カプセル化されたデータを取り出すための制御情報である第２利用制御情報を文書データに含まれる管理用識別子内に埋め込んだ構造化文書のデータ利用装置であって、配布される文書データの文書構造を解析する文書構造解析手段と、文書データに含まれる管理情報格納用データ内の第１利用制御情報を抽出する手段と、文書データに含まれる管理用識別子内の第２利用制御情報を抽出する第２利用制御情報抽出手段と、第２利用制御情報と、文書データに含まれる管理情報格納用データ内の第１利用制御情報とに基づいて、文書データの利用を許可あるいは制限する文書データ利用手段とを備える。
【０００８】
さらに、本発明に係る文書データ利用装置は、テキストデータ、画像データ、音楽データ、その他の電子化データで構成される文書データの利用を許可あるいは制限するために必要となる利用制御情報を相補的に構成する第１利用制御情報と第２利用制御情報とを生成し、文書データに対して複数の情報項目毎に識別子を設定し、識別子内に情報項目毎の内容情報を格納するとともに、文書データに含まれる管理情報格納用データ内に文書デー

タの一部を切り取ったものである第１利用制御情報を埋め込み、文書データ中の第１利用制御情報の位置情報である第２利用制御情報を文書データに含まれる管理用識別子内に埋め込んだ構造化文書のデータ利用装置であって、配布される文書データの文書構造を解析する文書構造解析手段と、文書データに含まれる管理情報格納用データ内の第１利用制御情報を抽出する手段と、文書データに含まれる管理用識別子内の第２利用制御情報を抽出する第２利用制御情報抽出手段と、第２利用制御情報と、文書データに含まれる管理情報格納用データ内の第１利用制御情報とに基づいて、文書データの利用を許可あるいは制限する文書データ利用手段とを備える。

【００１６】

【発明の実施の形態】

本発明の実施形態について、以下に説明する。

〔文書データ生成装置〕

文書データを配布する発行者側では、図１に示すような文書データ生成装置１００を用いて構造化文書を作成する。

文書データ生成装置１００は、各種データを入力するためのデータ入力部１０１、認証データやアクセス制限データを管理し認証データ管理ＤＢ１０３の内容を更新する認証・アクセス制限部１０２を備えている。また、文書データ生成装置１００は、データの暗号化および署名データを作成する暗号・署名部１０４、可視的な電子透かしデータまたは不可視の電子透かしデータを作成し電子化データに埋め込むための透かし埋込部１０５を備えている。さらに、文書データ生成装置１００は、XMLやHTMLなどの構造化文書における文書構造を生成するための文書構造生成部１０６および管理情報を生成し画像データを加工するための管理情報生成／画像加工部１０７を備えている。

【００１７】

文書データ生成装置１００は、テキストデータを管理する電子書類ＤＢ１０９および画像データを管理する電子書類１１０から電子化データを呼び出し、データ入力部１０１から入力される各種データに基づいて認証情報やアクセス制限情報などの認証データを生成し、文書データの利用制御情報を生成する。

利用制御情報のうちの一部は第１利用制御情報として必要に応じて暗号・署名部１０４によって暗号化され、透かし埋込部１０５によって不可視の電子透かしデータに変換され、電子書類１１０から得られる画像データに埋め込まれる。

【００１８】

電子書類１０９から得られるテキストデータおよび電子書類１１０から得られる画像データは、それぞれXML形式またはHTML形式などに基づいて、情報項目毎にタグが設定され、各タグの要素または属性としてその内容情報が格納される。

設定されたタグのタグ定義情報は、タグ定義ＤＢ１０８に格納される。

同時に、透かし埋込部１０５によって画像データに埋め込まれた不可視の電子透かしデータに基づく制御情報が、第１利用制御情報と相補的に利用制御情報を構成する第２利用制御情報として管理情報生成／画像加工部１０７によって生成される。この第２利用制御情報は、XML形式やHTML形式などの構造化文書におけるタグが設定され、このタグ内の要素または属性として内容情報が格納される。

ここでも、設定されたタグのタグ定義情報は、タグ定義ＤＢ１０８に格納される。

【００１９】

〔文書データ利用装置〕

配布された文書データを利用者が利用するために必要となる文書データ利用装置の概略構成を図２に示す。

文書データ利用装置２００は、各種データを入力するためのデータ入力部２０１、文書データの電子化データ内に埋め込まれた透かしデータを抽出するための透かし抽出部２０２、文書データ内に暗号化されたデータや署名情報が存在する場合にはこれらデータを復号化し、また署名データを復元するための復号・署名処理部２０３、認証情報やアクセス制限情報を解析しこれを認証データ管理ＤＢ２０５に格納する認証・アクセス制御管理部、

配布された文書データの構造解析を行ってタグ定義管理ＤＢ２０７に格納する文書構造解析部２０６、文書データを利用者に利用させるためのデータ利用部２０８などを備えている。

【００２０】

〔構造化文書〕

文書構造生成部１０６および管理情報生成／画像加工部１０７によって定義されたタグに基づいて、たとえば、図３に示すような構造化文書が生成される。

文書データの情報項目として選択されるテキスト情報１、画像情報１・・・テキスト情報２は、それぞれタグ１、タグ２・・・タグｎの識別子が付与され、各タグ内の要素としてその情報内容が格納される。

管理情報格納用データとして画像情報spが指定されると、これを文書データの情報項目として設定するためのタグspが設定され、このタグspの要素として情報内容が格納される。

【００２１】

タグ１～タグｎおよびタグspの要素として格納される各内容情報は、それぞれ各タグの属性として格納することも可能である。

タグspは格納される内容情報に応じて、複数の下位のタグを有する階層化された構造とすることができ、たとえば、図４に示すように、タグspの下位に複数のタグsp1、タグsp2・・・を含むような構成とすることができる。また、タグspは複数の属性を備える構造とすることができ、図５に示すように、タグspの属性として、属性１、属性２・・・を含むような構成とすることができる。

【００２２】

図４に示すように複数のタグでなるタグspを構成した場合には、各タグの要素を図６に示すように設定することができる。ここでは、タグsp1として改竄検出対象範囲、タグsp2として画像に記録している情報種別、タグsp3として暗号／認証／署名アルゴリズム種別、タグsp4として画像情報spアクセスポリシーが設定される。

タグsp1において設定する改竄検出対象範囲としては、文書データの各情報項目に設定されたタグを指定することで、そのタグの内容情報を改竄検出対象範囲として指定することが可能であり、たとえば、図６のタグ要素内容１では全タグを改竄検出対象範囲として指定し、タグ要素内容２ではタグ１およびタグ２のみを改竄検出対象範囲として指定している。

【００２３】

タグsp2において設定する画像に記録している情報種別は、電子透かしとして埋め込まれている第１利用制御情報の種別を示すものであり、署名データ、認証データ、暗号鍵、その他の情報種別のうちいずれであるかを記述する。また、タグsp2には、第１利用制御情報の構成、パラメータの指定、この文書データの配布経路を示す経路情報などを格納するように設定することもできる。

タグsp3に格納される暗号／認証／署名アルゴリズム種別情報は、不可視の電子透かしとして埋め込まれている第１利用制御情報が暗号化されている場合、その暗号鍵の種別、認証情報の認証方法に関するアルゴリズム、署名情報の認証方法に関するアルゴリズムなどを格納するように構成できる。

【００２４】

タグsp4として格納される画像情報spアクセスポリシーは、アクセス許可の制限に関する情報を設定するように構成でき、たとえば、図６に示すように、今日だけ閲覧することを許可する、日を問わず閲覧を許可するなどの種々の設定が可能である。

タグsp1～タグsp4の設定は図示したものに限定されるものではなく、５以上のタグを設定することも可能であり、３以下に設定することも可能であり、また、タグ内に複数の属性を含むような構成とすることも可能である。

【００２５】

図５に示すように複数の属性を備えるタグspを構成した場合には、各属性を図７に示すように設定することができる。ここでは、属性１として改竄検出対象範囲、属性２として画

像に記録している情報種別、属性３として暗号／認証／署名アルゴリズム種別、属性４として画像情報spアクセスポリシーが設定される。各属性１～属性４に設定されるデータは、複数のタグsp1～sp4で設定する場合と同様であり、ここでは説明を省略する。
タグspの下位に複数のタグsp1、タグsp2・・・を設定する場合のそれぞれのタグ名およびタグsp内に複数の属性１、属性２・・・を有する構成とする場合のそれぞれの属性名は、図８に示すようなタグ名または属性名とすることができる。

【００２６】

たとえば、透かし処理に関するパラメータを記述する場合には、そのタグ名を<透かし制御>とすることができる。図８に示すように、第１利用制御情報の透かし制御情報が「透かし埋込」である場合には、
<透かし制御>属性＝ENBED</透かし制御>
と記述し、第１利用制御情報の透かし制御が「透かし種別１：攻撃耐性強モード」である場合には、
<透かし制御>属性=1-SO</透かし制御>
と記述することができる。

【００２７】

この透かし制御をタグspの属性として記述する場合には、
<タグsp　透かし制御='EMBED'　/タグsp>
<タグsp　透かし制御='1-SO'　/タグsp>
と記述することができる。
また、不可視の透かしデータが埋め込まれたデータ名をタグの要素として記述する場合には、そのタグ名を<透かし対象名>とし、その要素として「透かし埋込／抽出対象ファイル名」を記述する。たとえば、図８に示す例では、Content1.jpgという画像データに透かしデータを埋め込んでいることを示すために、
<透かし対象名>Content1.jpg</透かし対象名>
と記述する。

【００２８】

同様に、この記述をタグspの属性として記述するには、
<タグsp　透かし対象名='Content1.jpg'　/タグsp>
と記述することができる。
第１利用制御情報として格納されている格納物の動作条件（制御プログラムのパラメータ）、格納物の指定（暗号化画像の指定）などのパラメータを指定する場合には、<パラメータ>というタグを設定することができる。たとえば、図８に示すように、
<パラメータ>プログラム名　属性=a</パラメータ>
<パラメータ>画像ファイル名</パラメータ>
と記述することができる。タグspの属性として各パラメータを設定する場合も、属性名として「パラメータ」を用いて記述することができる。

【００２９】

また、第１利用制御情報のデータ格納種別を<構成>というタグ名のタグで設定することができる。この構成タグは、各種管理情報を格納した複数のデータの構造体中に第１利用制御情報を格納した画像データが含まれている場合に、その構造体のデータ形式およびどのデータに第１利用制御情報が埋め込まれているかを示す。たとえば、図９に示すように、画像情報spが、JPG、BMP、GIF、その他のデータ形式でなる画像データを含むデータ１および暗号化画像、認証・暗号データ、制御プログラムなどの各種管理情報を格納する拡張部を含むデータ２が合成されたデータである場合、データ形式と第１利用制御情報が埋め込まれているデータを<構成>タグ内に記述する。たとえば、図８に示すように、
<構成>データ格納１</構成>
データ形式による書式
<タグ１>データ構成　属性=データ格納１</タグ１>
のように記述できる。

【００３０】
〔画像情報sp〕
図９に示すように、管理情報格納用データとして指定される画像情報sp１０は実際に表示される画像データが格納される第１データ部１１と、暗号化画像データや制御プログラムなどが格納される拡張部としての第２データ部１２とを含む構成とすることができる。
画像情報sp１０は、JPG，BMP，GIF，その他の画像データ形式で構成されており、暗号化画像データ、認証データ、暗号鍵情報、制御プログラムなどの利用制御情報が格納される。
【００３１】
画像情報sp１０内に第１利用制御情報を格納する方法を、図３０～図３３に示す。
図３０に示すように、第１利用制御情報を電子透かしとして画像情報sp１０の第１データ部１１に埋め込むように構成できる。ここでは、ステップＳ１７１において、第１利用制御情報を電子透かしとして画像情報sp１０の第１データ部１１に埋め込んでいる。
第１データ部１１に格納される画像データはモニタなどに実際に表示される画像データであるため、第１利用制御情報を秘匿情報とする場合には、不可視の電子透かしとして埋め込む必要がある。
【００３２】
図３１に示すように、第１利用制御情報を画像情報spの第２データ部１２に格納するように構成することができる。この場合、ステップＳ１８１において、第１利用制御情報を画像情報sp１０の第２データ部１２に格納している。第１利用制御情報は、不可視の透かしデータまたは可視的な透かしデータとして、第２データ部１２の画像フォーマットの冗長部に格納するように構成できる。
図３２に示すように、第１利用制御情報を暗号化して画像情報sp１０内に格納することができる。
【００３３】
まず、ステップＳ１９１において、第１利用制御情報を暗号化する。ここでの暗号鍵は、秘密鍵暗号系における共通鍵を用いて第１利用制御情報を暗号化することで、第１利用制御情報を秘匿情報とすることができる。また、第１利用制御情報が署名情報である場合には、公開鍵暗号系の秘密鍵を用いて暗号化することができる。
ステップＳ１９２では、第１利用制御情報を暗号化した暗号化情報を第２データ部１２に格納する。ここでは、第２データ部１２の画像フォーマットの冗長部に暗号化情報を不可視の透かしデータまたは可視的な透かしデータとして埋め込む。
【００３４】
ステップＳ１９３では、第１利用制御情報を暗号化した際に用いた暗号鍵を第１データ部１１に埋め込む。ここの場合も第１データ部１１は可視的な画像データであるため、暗号鍵を不可視の透かしデータとして第１データ部１１に埋め込むことで、暗号鍵を秘匿情報として格納することができる。第１利用制御情報を公開鍵暗号系の秘密鍵で暗号化した場合には、暗号鍵を第１データ部１１に埋め込む必要はない。
図３３のステップＳ２０１に示すように、第１利用制御情報を分離して第１データ部１１と第２データ部１２に格納するように構成できる。
【００３５】
たとえば、図３４に示すように、第１データ部１１に格納するためのデータ１と、第１利用制御情報から分離されたデータ1x、データ2xとを用意する。ステップＳ４０１において、データ1xを不可視の透かしデータとしてデータ１に埋め込む。ステップＳ４０２において、データ1xおよびデータ2xを用いてデータ変換を行いデータ２を生成する。ここでは、データ1xを用いてデータ2xを暗号化するなどのデータ変換処理が可能である。
ステップＳ４０３では、データ1xが埋め込まれたデータ１を画像情報sp１０の第１データ部１１に格納し、データ1xとデータ2xを用いてデータ変換されたデータ２を第２データ部１２に格納する。
【００３６】

このようにして画像情報sp１０内に格納された第１利用制御情報を復元するためのフローチャートを図３５に示す。ステップＳ４１１では、画像情報sp１０の第１データ部１１のデータから不可視の透かしデータとして埋め込まれているデータ1xを抽出する。ステップＳ４１２では、抽出したデータ1xと、第２データ部１２に格納されているデータ２とに基づいて、データ2xを復号化する。たとえば、データ1xを秘密鍵としてデータ2xが暗号化されている場合には、透かしデータから抽出されたデータ1xを用いてデータ2xを復号化する。

【００３７】

（画像情報spのデータ形式）

図４１に示すように、データ（１）で示されるような管理情報格納用画像データは、画像情報sp１０の第１データ部１１、第２データ部１２から構成されるデータ形式とし、下記データを格納する。

管理情報格納画像サイズが大きく、署名、timestamp、アクセスポリシーなどの透かし情報全てを透かし化可能な場合、画像情報sp１０の第１データ部１１に情報を格納する。また、管理情報格納用画像サイズが小さく、情報量が大きいプログラム等を透かし化できない場合、画像情報sp１０の第１データ部１１と第２データ部１２に分離して格納する。

【００３８】

画像情報sp１０の第１データ部１１、または第１データ部１１と第２データ部１２に分離して格納されるデータは、図４０に示すようなものが考えられる。

たとえば、全体データ（０）の特徴情報として、ハッシュ値などの署名情報、発行日などを示すtimestampなどを格納することができる。また、データ（１）の特徴情報として、ハッシュ値などの署名情報、発行日や更新日を示すtimestampを格納でき、データ（１）のアクセスポリシーとして、利用者名、利用許諾期間、リードオンリーや変更許諾などの読み書きの許諾情報などを格納することができる。さらに、データ（２）の特徴情報として、ハッシュ値など署名情報、部分文字、発行日や更新日を示すtimestampなどを格納でき、データ（２）のアクセスポリシーとして利用者名、利用許諾期間、読み書きに対する許諾情報、権利者ＩＤ、住所・電話番号・URLなどの連絡先情報、利用許可回数などを格納することができる。さらに、JAVA（登録商標）アプリケーションなどのプログラムを格納することも可能である。

【００３９】

〔電子文書生成フロー〕

（署名処理文書の生成）

デジタル署名をした文書データを生成する場合のフローチャートを図１２に示す。

ステップＳ３１では、改竄検出範囲の対象となるエレメントを指定する。たとえば、データ入力部１０１からの入力を受け付けて、文書データに含まれる情報項目を指定させることによりどのエレメントを改竄検出範囲の対象とするかを決定する。文書データに含まれる電子化データのファイル名などにより予め改竄検出範囲の対象に設定されているエレメントがある場合には、自動的にそれを改竄検出範囲の対象に設定することもできる。

【００４０】

ステップＳ３２では、改竄検出範囲の対象となるエレメントのデジタル署名を行う。たとえば、改竄検出範囲の対象となったエレメント全体のハッシュ値を算出し、これを署名情報として保存する。

ステップＳ３３では、文書データ中から変換対象エレメントを選択する。ここでは、画像情報spとして変換する変換対象エレメントの選択を受け付ける。

ステップＳ３４では、選択した変換対象エレメントに対して変換処理を実行する。変換対象エレメントに対する変換ルールは、予め設定された変換ルールを採用することも可能であり、データ入力部１０１から入力される変換ルールを採用することも可能である。

【００４１】

ステップＳ３５では、変換対象エレメントと署名情報とを画像データに記録する。このとき、変換対象エレメントは原情報であり、この原情報と署名情報とを不可視の電子透かし

として画像データに埋め込む。
（署名処理文書の利用）
デジタル署名処理がなされた文書データを利用する場合のフローチャートを図１３に示す。
ステップＳ４１では、改竄検出範囲の対象となるエレメントを指定する。ここでは、文書の構造解析を行って、タグsp内の情報から改竄検出範囲の対象となっているエレメントを検出することで、改竄検出範囲の対象であるエレメントを指定することができる。
【００４２】
ステップＳ４２では変換対象エレメントを選択する。タグsp内の情報から変換対象エレメントの情報を取得しこれを変換対象エレメントとする。
ステップＳ４３では、変換エレメントの復元を行う。たとえば、画像情報sp内に埋め込まれた変換対象エレメントに対応する原情報を抽出する。
ステップＳ４４では、改竄検出範囲の対象であるエレメントの検証を行う。タグsp内の情報から改竄検出範囲の対象となっているエレメントを抽出し、この署名情報を生成する。たとえば、改竄検出範囲の対象となっているエレメント全体のハッシュ値を算出し、これと画像情報sp中から復元された署名情報とを検証する。
【００４３】
（署名情報の検証）
XML文書など構造化文書を用いて署名情報を生成する方法を図３８のフローチャートに示す。
ステップＳ２３１では、文書データのうちからデジタル署名を行う署名範囲を指定し、この指定範囲をタグsp内に記述する。署名範囲は、文書データ中のタグを選択することで指定することが可能である。また、署名範囲の情報内容をタグsp内の要素または属性として記述することで、署名範囲を特定することができる。
【００４４】
ステップＳ２３２では、指定された署名範囲の署名情報（ｓ）を生成する。ここでは、署名範囲に含まれる全エレメントのハッシュ値を算出することで、署名情報（ｓ）を生成する。
ステップＳ２３３では、署名情報（ｓ）を画像情報sp内に透かし情報として埋め込む。
配布された文書データの署名情報を検証するためのフローチャートを図３９に示す。
【００４５】
ステップＳ２４１では、構造化文書を解析し、タグspの要素または属性内に含まれる署名範囲に関する情報を取得する。
ステップＳ２４２では、取得した署名範囲内の署名情報（s0）を生成する。ここでは、現在の文書データの署名範囲に含まれる全エレメントのハッシュ値を算出することで、署名情報（s0）を生成する。
ステップＳ２４３では、画像情報spに含まれる透かしデータを抽出し、透かしデータに含まれる署名情報（s1）を抽出する。
【００４６】
ステップＳ２４４では、署名情報の検証を行う。ここでは、現在の文書データから求められた署名情報（s0）と、透かしデータから抽出した署名情報（s1）とを比較し、一致していれば検証成功とし、一致していない場合には検証失敗としてエラー処理を行う。
（秘匿処理文書の生成）
文書データ生成装置１００によって一部を秘匿情報とした文書データを作成する場合の制御フローチャートを図１０に示す。
【００４７】
ステップＳ１１では、改竄検出対象のエレメントを指定する。ここでは、データ入力部１０１から入力される情報に基づいて、文書データに配置される各エレメントのうちどのエレメントを改竄検出対象とするかを決定する。
ステップＳ１２では、改竄検出範囲の対象となるエレメントを署名する。たとえば、改竄

検出範囲の対象となったエレメント全体のハッシュ値を算出し、これを署名値として保存する。
ステップＳ１３では、変換対象エレメントを選択する。ここでは管理情報として変換する変換対象エレメントを選択するもので、たとえば、文書データ中の一部を秘匿情報としこれを他の特定情報と置き換えて配布するような場合、この秘匿対象情報を変換対象エレメントとして選択するように構成できる。変換対象エレメントの選択方法は、予め設定される変換対象エレメントまたはデータ入力部１０１から入力される情報に基づいて決定することができる。
【００４８】
ステップＳ１４では、選択した変換対象エレメントに対して変換処理を実行する。変換対象エレメントに対する変換ルールは、予め設定された変換ルールを採用することも可能であり、データ入力部１０１から入力される変換ルールを採用することも可能である。
ステップＳ１５では、入力される認証情報に基づいて認証情報の設定を行う。
認証情報は、公開鍵暗号系の秘密鍵、共通鍵暗号系の共通鍵、利用者の個人情報、記録される媒体の識別情報、その他の認証情報を選択することが可能であり、データ入力部１０１から入力される情報を採用することができる。
【００４９】
ステップＳ１６では、設定された認証情報を用いて変換対象エレメントを暗号化する。暗号化方法は、種々の暗号化方法を利用することが可能であり、正当な利用者が復号化して利用することが可能な方法での暗号化が実行される。
ステップＳ１７では、変換対象エレメントを特定情報で置き換える。ここでは、秘匿情報となる変換対象エレメントに代わる特定情報を変換対象エレメントの位置に配置する。
ステップＳ１８では、暗号化された変換対象エレメント、署名情報、認証情報を文書データに含まれる画像データに不可視の透かし情報として埋め込む。たとえば、変換対象エレメントを共通鍵暗号系の共通鍵で暗号化した場合には、変換対象エレメントの暗号化情報、共通鍵情報、改竄検出範囲の対象となるエレメントの署名値などを不可視の透かしデータとして画像データに埋め込む。変換対象エレメントとして画像データの一部を選択した場合には、画像データ中の変換対象エレメントに相当する部分が他の特定情報に変換されて表示されるように置き換えられ、原情報の変換対象エレメント部分は暗号化されて暗号鍵とともに透かしデータとして画像データ内に埋め込まれる。
【００５０】
（秘匿処理文書の利用）
一部を秘匿情報として含む文書データを利用するためのフローチャートを図１１に示す。
ステップＳ２１では、改竄検出対象のエレメントを指定する。文書の構造解析を行って、タグsp内の情報から改竄検出範囲の対象となっているエレメントを検出し、これを改竄検出対象のエレメントとして指定する。
ステップＳ２２では画像データから認証情報を取得する。画像データに不可視の透かしデータとして埋め込まれている第１利用制御情報を抽出し、これに含まれている認証情報を取得する。
【００５１】
ステップＳ２３では、利用者が入力する認証情報を受け付けて、これを第１利用制御情報から抽出した認証情報と比較する。たとえば、利用者の個人情報や記録媒体の識別情報などを利用者に入力させ、これを第１利用制御情報から抽出した認証情報と比較し、一致しなければ処理を中止する。
ステップＳ２４では、変換対象エレメントを選択する。ここでは、文書データ中に含まれる暗号化データを指定し変換対象エレメントとする。
ステップＳ２５では、認証情報を用いて変換対象エレメントを復号化する。
【００５２】
ステップＳ２６では、復号化された変換対象エレメントを用いて電子化データの復元を行う。

ステップＳ２７では、改竄検出範囲の対象となっているエレメントの検証を行う。たとえば、復元された電子化データを含む文書データ内の改竄検出範囲に対してハッシュ値を求め、第１利用制御情報に含まれる原情報のハッシュとの比較を行うことで改竄があったか否かを検証する。

（秘匿処理文書の検証）

XML文書など構造化文書を用いて秘匿処理情報を生成する方法を図３６のフローチャートに示す。

【００５３】

ステップＳ２１１では、情報（a0）を構造化文書に記録する。たとえば、タグsp中に設定されるタグまたはタグsp中の属性に情報（a0）を記述するか、あるいは、文書データ中のタグで情報（a0）を指定するように設定することで情報（a0）を構造化文書に記録することができる。

ステップＳ２１２では、情報（a0）の複製情報（a1）を透かしデータとして画像情報sp中に埋め込み、透かしデータを抽出するためのデータをタグsp中に記述する。

【００５４】

配布された文書データの秘匿情報を検証するためのフローチャートを図３７に示す。

ステップＳ２２１では、構造化文書を解析し、情報（a0）を取り出す。ここでは、タグspの要素または属性内に含まれる情報に基づいて情報（a0）を取得する。

ステップＳ２２２では、透かしデータから情報（a1）を抽出する。ここでは、タグspの情報を解析することにより透かし制御情報を取得し、これに基づいて透かしデータから情報（a1）を抽出する。

【００５５】

ステップＳ２２３では、構造化文書中の情報（a0）と透かしデータから抽出した情報（a1）とを比較し検証を行う。構造化文書中の情報（a0）と透かしデータから抽出した情報（a1）とが一致した場合には検証成功とし、一致していない場合には検証失敗としてエラー処理を行う。

（構造化文書タグの生成）

配布する文書データをXMLやHTMLなどの構造化文書とする場合に文書タグを生成するフローチャートを図１４に示す。

【００５６】

ステップＳ５１では、文書データに含まれる電子化データについて、情報項目別にタグ（１～ｎ）を設定し、各タグ（１～ｎ）内の情報内容であるエレメント（１～ｎ）を生成する。

ステップＳ５２では、管理情報格納用データである画像情報spに関する情報を格納するためのタグspを生成する。

ステップＳ５３では、タグsp内に設定される複数のタグ（sp1,sp2・・・）または属性（１，２・・・）の設定を行う。前述したように、第２利用制御情報として、図６に示すような複数のタグまたは図７に示すような複数の属性を設定することができる。

【００５７】

ステップＳ５４では、画像情報spを指定する。ここでは、第１利用制御情報が格納される画像情報spを指定する。

ステップＳ５５では、画像情報spに格納する第１利用制御情報を生成し、この第１利用制御情報を画像情報sp内に格納するとともに、第１利用制御情報を画像情報spから抽出して、第１利用制御情報とともに文書データを利用させるための第２利用制御情報をタグsp内に格納する。

（構造化文書タグの利用）

配布された構造化文書を利用する際のタグ解析方法のフローチャートを図１５に示す。

【００５８】

ステップＳ６１では、タグ（１～ｎ，sp）およびエレメント（１～ｎ，sp）を入力する。ここでは、配布された構造化文書中の各タグ（１～ｎ，sp）の構造解析を行い、同時に各

タグ内の要素を取り込む。
ステップＳ６２では、タグspの解析を行う。タグspには画像情報spに関する情報（第２利用制御情報）が格納されており、タグspの解析を行うことで、画像データ内に格納されている第１利用制御情報を引き出すことができる。
ステップＳ６３では、画像情報spを解析し、情報復元／検証を行う。タグspに格納されている第２利用制御情報に基づいて、画像データ中に含まれる第１利用制御情報を抽出し、暗号化データを復号化したり、署名情報、秘匿情報の検証を行う。
【００５９】
ステップＳ６４では、復元エレメントの表示を行う。ここでは、XML文書やHTML文書などの構造化文書データを、その文書データ内で指定するスタイルシートに基づいて表示する。
（アクセスポリシー）
アクセスポリシーを利用制御情報とする場合のデータ例を図１８に示す。
アクセスポリシーは、たとえば、図１８に示すように、有効期限、残利用回数、利用者属性、処理権限、その他のポリシー種別に分けることができる。
【００６０】
アクセスポリシーとして有効期限を設定する場合には、たとえば、図１８に示すように、「～YY.MM.DD」、「Forever」、「TODAY」などの期限を示すデータを内容情報とすることができる。また、アクセスポリシーとして残利用回数を設定する場合には、設定される初期値から利用する毎にカウントダウンされる残利用回数を内容情報とすることができる。
アクセスポリシーとして利用者属性を設定する場合には、「個人利用のみの許可（+S）」、「グループ利用を許可する（+G）」などのデータを内容情報とすることができる。アクセスポリシーとして処理権限を設定する場合には、「読むだけ（+R）」、「書換可能（+W）」、「追記可能（+A）」などのデータを内容情報とすることができる。
【００６１】
（アクセスポリシーに対する文書タグ生成）
アクセスポリシーをタグspに設定する場合の文書タグ生成のフローチャートを図１６に示す。
ステップＳ７１では、アクセスポリシーの指定を行う。たとえば、有効期限、残利用回数、利用者属性、処理権限のうちの１または複数のアクセスポリシー種別とそのアクセスポリシー種別に設定されるポリシー内容を決定する。
ステップＳ７２では、アクセスポリシーをタグspに格納する。たとえば、タグsp中のタグsp4をアクセスポリシーのタグに設定し、タグsp4の要素としてポリシー内容を格納するように構成できる。アクセスポリシーの内容情報をタグspの属性として記述することも可能である。
【００６２】
ステップＳ７３では、画像情報spを指定する。ここでは、アクセスポリシーのポリシー内容を第１利用制御情報として埋め込むための画像情報spを決定する。
ステップＳ７４では、アクセスポリシーの内容情報を画像情報spに格納する。
ここでは、アクセスポリシーとして設定された内容情報を不可視の電子透かしデータとして画像情報spに埋め込む。
（アクセスポリシーのタグ利用）
アクセスポリシーが利用制御情報として設定された文書データを利用する際のフローチャートを図１７に示す。
【００６３】
ステップＳ８１では、配布された文書データからタグを解析する。
ステップＳ８２では、タグの解析結果に基づいて、タグsp内に格納されたアクセスポリシーの内容情報（p0）を取得する。
ステップＳ８３では、不可視の透かしデータとして画像情報spに埋め込まれたアクセスポリシーの内容情報（p1）を抽出する。

ステップＳ８４では、タグsp内に格納されていたアクセスポリシーの内容情報（P0）と、画像情報spから抽出したアクセスポリシーの内容情報（p1）とを比較し、一致するか否かを判別する。タグsp内に格納されていたアクセスポリシーの内容情報（P0）と、画像情報spから抽出したアクセスポリシーの内容情報（p1）とが一致した場合には、ステップＳ８５に移行する。

【００６４】

ステップＳ８５では、アクセスポリシーに基づいて利用者に文書データを利用させる。たとえば、アクセスポリシーの内容情報が"+R+Today"であれば、「今日だけ読むだけ」の制限の下に文書データを利用させる。また、アクセスポリシーとして残利用回数設定がなされている場合には、現在の残利用回数をカウントダウンしてアクセスポリシーの内容情報を更新し、タグsp内のアクセスポリシーの内容情報を変更するとともに、新たなアクセスポリシーの内容情報を画像情報spに不可視の透かしデータとして埋め込む。

【００６５】

（流通経路情報）

流通経路情報を利用制御情報として設定する場合には、たとえば、図２１に示すようなデータを採用することができる。ここでは、流通元となる経路（From）、流通途中の経路１（Through）および経路２（Through）、流通先となる経路（To）などを設定でき、各経路のデータとしては、たとえば、URL情報、MACアドレス情報、端末情報などの形式で表示することができる。

（流通経路情報に対するタグ生成）

流通経路情報をタグとして設定して文書データを生成する場合のフローチャートを図１９に示す。

【００６６】

ステップＳ９１では、流通元となる経路（From）、流通途中の経路（Through）、流通先となる経路（To）のうちいずれの流通経路であるかを指定する。

ステップＳ９２では、流通経路の種別情報をタグsp内のタグ名として設定し、そのタグの内容情報としてURLやMACアドレスなどの識別情報を第２利用制御情報として格納する。

ステップＳ９３では、流通経路情報を第１利用制御情報として格納するための画像情報spを指定する。

【００６７】

ステップＳ９４では、流通経路情報を画像情報spに格納する。このとき、流通経路情報を不可視の電子透かしデータとして画像情報spに埋め込むことができる。

（流通経路情報のタグ利用）

流通経路情報が利用制御情報として設定された文書データを利用する際のフローチャートを図２０に示す。

ステップＳ１０１では、配布された文書データからタグを解析する。

【００６８】

ステップＳ１０２では、タグの解析結果に基づいて、タグsp内に格納された流通経路情報の内容情報を取得する。

ステップＳ１０３では、不可視の透かしデータとして画像spに埋め込まれた利用端末経路情報を抽出する。

ステップＳ１０４では、タグsp内に格納されていた流通経路情報と、画像情報spから抽出した利用端末経路情報とを比較し、一致するか否かを判別する。タグsp内に格納されていた流通経路情報と、画像情報spから抽出した利用端末経路情報とが一致した場合には、ステップＳ１０５に移行し、一致しなかった場合にはステップＳ１０６に移行する。

【００６９】

ステップＳ１０５では、画像情報spから抽出した利用端末経路情報中の経路（From）宛てに確認情報を送出する。

ステップＳ１０６では、画像情報spから抽出した利用端末経路情報中の経路（From）宛てにＮＧ情報を送出する。

（プログラム制御を行う文書データの生成）
画像情報sp中にプログラムが格納されており、この文書データを利用する際にプログラムが起動し、設定されたパラメータに応じた処理を実行するように構成することができる。このような文書データを生成する際のフローチャートを図２２に示す。
【００７０】
ステップＳ１１１では、文書データに対してプログラムにどのような処理を実行させるかのパラメータによる機能設定を行う。
ステップＳ１１２では、設定されたパラメータ値を第２利用制御情報としてタグsp内に格納する。
ステップＳ１１３では、プログラムデータを生成する。ここでは、文書データを利用する際に、設定されるパラメータに応じた処理を実行するためのプログラムデータを生成する。
【００７１】
ステップＳ１１４では、画像情報spとして電子化データを指定する。ここでは、文書データ中の電子化データあるいは他の電子化データを選択することが可能である。
ステップＳ１１５では、プログラムデータおよび設定されたパラメータを画像情報sp内に格納する。ここでは、プログラムデータおよびパラメータ値を画像情報sp中に不可視の透かしデータとして格納することが可能であり、また、プログラムデータを暗号化して画像情報spの拡張部に格納することも可能である。
【００７２】
（プログラム制御を行う文書データの利用）
画像情報sp中にプログラムが格納された文書データを利用する際のフローチャートを図２３に示す。
ステップＳ１２１では、プログラムパラメータを取得する。プログラムパラメータは、タグsp中に格納された情報から取得することが可能であり、また画像情報spに透かし情報として埋め込まれた情報から取得することも可能であり、両者を比較して改竄があったか否かを検証するように構成することも可能である。
【００７３】
ステップＳ１２２では、画像情報spからプログラムデータを読み出す。プログラムデータが画像情報spに透かしデータとして埋め込まれている場合にはこれを抽出することをプログラムデータの読出を行うことができる。また、プログラムデータが暗号化されている場合には、暗号鍵を用いて復号化を行う。暗号鍵は画像情報sp内に不可視透かしとして格納されている場合、利用者の識別情報などを用いる場合など種々の場合があり、それぞれの場合に応じて適切な暗号鍵を用いて復号化を行う。
【００７４】
ステップＳ１２３では、読み出したプログラムを起動する。
ステップＳ１２４では、パラメータを入力する。ここでは、ステップＳ１２１で取得したパラメータをプログラムに入力する。
ステップＳ１２５では、入力されたパラメータの判別を行う。たとえば、入力されたパラメータが'a'であればステップＳ１２６に移行して処理Ａを実行し、そうでない場合にはステップＳ１２７に移行して処理Ｂを実行する。
（暗号化画像を含む文書データの生成）
暗号化画像を含む文書データを生成する際のフローチャートを図２４に示す。
【００７５】
ステップＳ１３１では、画像データを暗号化するための暗号鍵を指定する。たとえば、共通鍵暗号系の秘密鍵として任意に選択される暗号鍵、利用者の識別情報、記録媒体の識別情報、その他の情報を暗号鍵とすることができる。
ステップＳ１３２では指定された暗号鍵を用いて画像データの暗号化を行う。
ステップＳ１３３では、パラメータの設定を行う。ここでは、暗号のアルゴリズムに関するパラメータをタグsp内に設定するとともに、画像情報sp内に格納する画像データの指定

を行うためのパラメータをタグsp内に設定する。
【００７６】
ステップＳ１３４では、設定されたパラメータ値をタグspに格納する。
ステップＳ１３５では、画像データのハッシュ値を生成する。ここでは暗号化後の画像データのハッシュ値を算出する。
ステップＳ１３６では、画像情報spとして電子化データを指定する。
ステップＳ１３７では、画像情報spに、画像データのハッシュ値、暗号化画像データ、暗号鍵などを格納する。暗号化画像データを画像情報spの拡張部に格納し、画像データのハッシュ値および暗号鍵を指定された電子化データに不可視の透かしデータとして埋め込むことが可能であり、双方を電子化データ内に不可視の透かしデータとして埋め込むことも可能である。
【００７７】
（暗号化画像を含む文書データの利用）
暗号化画像データを含む文書データを利用する際のフローチャートを図２５に示す。
ステップＳ１４１では、タグspに格納されている情報に基づいてパラメータを取得する。ここでは、暗号アルゴリズムおよび暗号化画像データを特定するためのパラメータを取得する。
ステップＳ１４２では、画像情報spから暗号鍵、暗号化画像データ、ハッシュ値（s0）を読み出す。タグspから取得したパラメータに基づいて、不可視の透かしデータとして電子化データ内に埋め込まれた暗号鍵およびハッシュ値を抽出し、画像情報spの拡張部に格納された暗号化画像データまたは電子化データに不可視の透かしデータとして埋め込まれた暗号化画像データを読み込む。
【００７８】
ステップＳ１４３では、読み出した暗号化画像データのハッシュ値（s1）を算出する。
ステップＳ１４４では、画像情報spから読み出したハッシュ値（s0）と算出された暗号化画像データのハッシュ値（s1）とを比較し、一致した場合にはステップＳ１４５に移行し、一致しなかった場合にはステップＳ１４７に移行する。
ステップＳ１４５では、暗号化画像データを読み出した暗号鍵を用いて復号化しステップＳ１４６において画像データを利用させる。
【００７９】
ステップＳ１４７では、データの改竄があったとみなしてエラー処理を実行し、処理を終了する。
暗号化画像データとしては、たとえば、図２７に示すように、画像情報spとして選択した印鑑の画像データ２１を用いることができる。この画像データ２１を暗号鍵を用いて暗号化し暗号化画像データ２２を生成する。この暗号化画像データ２２を不可視の透かしデータとして画像データ２１と重ね合わせて画像情報spとして格納する。
【００８０】
配布された文書データを利用する前は、暗号化画像データ２２が不可視の透かしデータとして埋め込まれているため、画像情報spは利用処理前画像データ２３として見かけ上印鑑の画像データとなっている。この画像情報spを利用する際には、画像データ２４と暗号化画像データ２５に分離され、ともに利用することが可能となる。
このような認証に用いられる画像データとしては、図２６に示すように、顔部（写真、イラスト）画像、サイン・署名、指紋画像などを用いることができる。
【００８１】
（紙書類の電子化管理）
上述のような方法を用いて紙書類を電子化して管理する場合を図４９に基づいて考察する。
紙書類５０１はスキャナーを用いて画像データ化して、たとえばビットマップデータ５０２とすることができる。このビットマップデータ５０２にアクセス制御／認証情報などの暗号化画像データが埋め込まれたアカウント画像５０３を合成し、ビットマップデータ５

０２およびアカウント画像５０３を含む文書データ５０４を構造化文書として作成する。
【００８２】
正当な権利者による利用であると判断される場合には、アカウント画像５０３を除去してビットマップデータ５０２の閲覧などを許可するようにする。
文書データ５０４の利用が終了した際に、文書データ５０４を利用した利用者データおよび利用日などの情報をアカウント画像５０３に埋め込まれる暗号化データに追加して、再度ビットマップデータ５０２と合成し管理することも可能である。
（電子化文書の認証情報の紙書類への反映）
文書の電子化が進んでいないような機関では、紙書類による管理を行っており、書類に記されたサインなどにより認証を行っている。たとえば、文書作成者の電子署名が付いた電子文書をインターネットを通じて海外に送信し、税関などの官庁に提出するための紙書類とする場合、書類にサインが記されていたとしても本人認証を行うことが困難である。このような場合に、文書作成者の認証を行うことが可能な文書加工の方法について、図６９に基づいて説明する。
【００８３】
ここでは、文書作成者または文書送信者が第１ユーザ端末８００からインターネット網８７０を介して文書提出者の第２ユーザ端末８２０に電子文書を送信する。送信する電子文書は、文書作成者の電子署名が付与された電子文書８０１であり、たとえば電子商取引文書を電子化したものを採用できる。
電子文書８０１は、第１ユーザ端末８００からインターネット網８７０を介して第２ユーザ端末８２０に送信される。
第２ユーザ端末８２０側では、受信した電子文書８２１（送信側における電子文書８０１と同一）をプリンタ８２２により紙書類として印刷し、紙文書８２３を作成する。このとき、文書作成者を認証するための電子署名などの秘匿情報をイメージスキャナーなどで読みとることが可能な電子透かし情報として紙文書８２３に印刷する。
【００８４】
このように作成された紙文書８２３は、文書管理機関８５０においてイメージスキャナで電子透かしを読みとることによって文書作成者の認証を行うことが可能となり、改竄などの不正が行われたか否かを判別することが可能となる。電子商取引文書を官庁に提出する場合には、文書提出者が印刷された電子商取引文書（紙文書８２３）を官庁（文書管理機関８５０）に提出し、官庁においてこの電子商取引文書の認証を行うことが可能となる。
（電子化データの管理）
同様にして、テキストデータなどの電子化データ５１１に対して、アクセス制御情報や認証情報が暗号化データとして埋め込まれたアカウント画像５１２を合成し、構造化文書形式による文書データ５１３を作成する。
【００８５】
この場合も、同様にして、正当な利用であると判断される場合に、アカウント画像５１２を除去または不可視化し、電子化データ５１１の閲覧などを許可する。また、利用終了後に、文書データ５１３の利用者および利用日などの情報をアカウント画像５１２に透かしデータとして埋め込んで、再度電子化データ５１１と合成して管理することも可能である。
（カプセル化情報を含む文章データの生成）
複数種類の利用制御情報をタグspおよび画像情報spに格納するようにした文書データの生成についてそのフローチャートを図２８に示す。
【００８６】
ステップＳ１５１では、画像情報spに格納する利用制御情報を指定する。たとえば、画像情報spに第１利用制御情報として格納するための暗号化データ、認証情報、暗号鍵情報、制御プログラム、その他の情報を指定する。
ステップＳ１５２では、各種パラメータの設定を行う。ここでは、タグspに格納する第２利用制御情報をパラメータとして設定する。

ステップＳ１５４では、署名対象情報の署名情報を生成する。ここでは、構造化文書データのデジタル署名をするために署名対象範囲を指定し、この署名対象範囲のエレメントのハッシュ値を算出することにより署名情報を生成する。

【００８７】

ステップＳ１５５では、画像情報spを指定する。管理画像となる電子化データを指定し、画像情報spに設定する。

ステップＳ１５６では、デジタル署名により算出された署名情報、その他の各種利用制御情報を画像情報spに格納する。

ステップＳ１５７では、各種パラメータ値を格納する。ここでは、画像情報spに格納される第１利用制御情報に対して設定された各種パラメータ値をタグsp内に格納する。

【００８８】

（カプセル化情報を含む文書データの利用）

複数種類の利用制御情報をタグspおよび画像情報spに格納した文書データの利用についてそのフローチャートを図２９に示す。

ステップＳ１６１では、各種パラメータ値を取得する。ここでは、タグspの情報を解析することにより、画像情報sp内に格納された第１利用制御情報に対する各種パラメータを取得する。

ステップＳ１６２では、画像情報spからカプセル化した各種情報を分離する。

たとえば、画像情報spに格納されている暗号化データ、認証情報、暗号鍵情報、制御プログラム、デジタル署名により算出された署名情報などを抽出する。

【００８９】

ステップＳ１６３では、署名情報を生成する。ここでは、文書データの署名範囲を各エレメントとし、署名情報を生成する。

ステップＳ１６４では、画像情報spから分離した署名情報と、現在の文書データに基づいて生成した署名情報とを比較する。署名対象範囲の署名情報が一致しなかった場合にはステップＳ１６５に移行し、各署名情報が一致した場合にはステップＳ１６６に移行する。

ステップＳ１６５では、エラー処理を実行し処理を終了する。

【００９０】

ステップＳ１６６では、秘匿情報の復号化を行う。たとえば、画像情報spから分離した暗号化データを、同じく画像情報spから分離した暗号化鍵を用いて復号化する。

秘匿情報に画像データを含む場合にはステップＳ１６７で画像データの復号化を行い、秘匿情報にテキストデータを含む場合にはステップＳ１６８においてテキストデータの復号化を行い、秘匿情報に音声情報を含む場合にはステップＳ１６９において音声データの復号化を行う。

【００９１】

ステップＳ１７０では、復号化された画像データ、テキストデータ、音声データを合成し、これを利用させる。

（ＯＳ登録画面との連携）

文書データの配布を行う発行者側のＯＳ（Operating System）側に利用者情報を登録しておき、画像情報spにこの利用者情報を格納して文書データを配布するように構成できる。

たとえば、発行者側のＯＳ４０６では、利用者Ａ，Ｂ・・・Ｘの利用者情報を管理しており、各利用者情報に基づいて生成されたＯＳ管理画像ファイル４０４、４０７、４０８を管理している。発行者側では、各種アプリケーションプログラム４０５を用いて画像ファイル４０２、その他の電子化データ４０３を生成し、ＯＳ４０６が管理している利用者Ａ用の管理画像ファイル４０４を用意し、これらに基づく文書データを配布する。

【００９２】

（ＯＳへの登録）

利用者情報に基づくＯＳ管理画像ファイルを登録する際のフローチャートを図４２に示す。

ステップＳ２５１では、利用者情報を入力する。この場合、利用者を特定するための利用

者ＩＤ、その利用者に対する許諾情報などの権利情報を入力する。
ステップＳ２５２では、利用者情報を画像データに記録する。ここでは、入力された利用者情報を不可視の透かしデータにするかあるいは暗号化して、画像データに記録する。画像データは発行者側で任意に選択したものを利用することができ、利用者が選択した画像データを用いることも可能である。
【００９３】
ステップＳ２５３では、画像データをファイル化する。ここでは、利用者情報が記録された画像データを、ＯＳ４０６が管理するデータベースのファイル形式に変換する。
ステップＳ２５４では、利用者情報を含む画像ファイルをＯＳ４０６が管理するデータベースに登録する。
（ＯＳ登録画像ファイルの利用）
ＯＳ４０６に登録された画像ファイルを利用する場合のフローチャートを図４３に示す。
【００９４】
ステップＳ２６１では、ＯＳを起動しログイン画面の表示を行う。
ステップＳ２６２では、パスワード入力を受け付け、認証を行う。
ステップＳ２６３では、画像ファイルに記録されているセキュリティ管理データをＯＳに登録する。
ステップＳ２６４では、文書データに画像情報spとして含まれる画像ファイルから透かしデータ、暗号化データ、暗号化鍵などのデータを取り出して、改竄検出、認証、アクセス制御などの処理を行う。
【００９５】
（ＯＳ登録画像を用いた文書データの生成）
ＯＳ登録画像を用いて文書データを生成する場合のフローチャートを図４５に示す。
ステップＳ２７１では、書類セキュリティ生成プログラムを開始する。
ステップＳ２７２では、画像情報spのデータ形式を指定する。たとえば、図４６に示すような、テキスト部３１、画像部３２および画像情報sp部３３を含む文書データ３０の場合を考える。画像情報３３のデータ形式は、図４７に示すような各種のデータ形式が考えられる。
【００９６】
Type１は、テキスト部３１および画像部３２の署名情報を生成し、これを不可視の透かし（データ1X）として画像データに埋め込むものである。また、署名対象情報をデータ拡張部に（データ2X）として格納する。
Type２は、テキスト部３１および画像部３２から署名情報を生成し、テキスト部３１の秘匿用暗号鍵と署名情報とを不可視透かし（データ1X）として画像データに埋め込み、署名／暗号化対象情報をデータ拡張部に（データ2X）として格納するものである。
【００９７】
Type３は、テキスト部３１および画像部３２から署名情報を生成し、署名情報を不可視透かし（データ1X）として画像データに埋め込み、署名／暗号化対象情報をテキスト部３１の秘匿用暗号鍵とを拡張部に（データ2X）として格納するものである。
Type４は、テキスト部３１および画像部３２から署名情報を生成し、テキスト部３１の秘匿用暗号鍵を不可視透かし（データ1X）として画像データに埋め込み、署名情報と署名／暗号化対象情報とを拡張部に（データ2X）として格納するものである。
【００９８】
ステップＳ２７４では、テキスト部３１および画像部３２から署名情報を生成する。
ステップＳ２７５では、暗号鍵Ｋの設定を行う。画像情報spのデータ形式がType１の場合には暗号鍵Ｋの設定を行う必要はなく、この場合にはこのステップＳ２７５をスキップする。
ステップＳ２７６では、画像情報spを選択する。ＯＳ登録画像を利用する場合にはステップＳ２７７に移行し、ＯＳ登録画像を利用しない場合にはステップＳ２７９に移行する。
【００９９】

ステップＳ２７７では、ＯＳ登録画像を取得する。ここでは、配布を行う利用者の利用者情報が設定されたＯＳ登録画像ファイルを呼び出してこれを画像情報spに設定する。
ステップＳ２７８では、画像情報spに各種情報を格納する。ステップＳ２７２で指定したデータ形式に応じて、画像情報spに各種情報を格納するものであって、図３０～図３５で説明した情報格納方法を用いて処理される。
ステップＳ２７９では、画像情報spとなる任意の画像データを選択し管理情報格納用データを生成する。
【０１００】
ステップＳ２８０では、画像情報spに各種情報を格納する。ここでも、ステップＳ２７８と同様にして、ステップＳ２７２で指定したデータ形式に応じて、画像情報spに各種情報を格納するものであって、図３０～図３５で示す情報格納方法を用いて処理することができる。
（ＯＳ登録画像を用いた文書データの利用）
配布される文書データがＯＳ登録画像を用いたものである場合の文書データの利用についてそのフローチャートを図４８に示す。
【０１０１】
ステップＳ２８１では、セキュリティ機能プログラムを起動させる。
ステップＳ２８２では、文書データの構造解析を行い、タグ情報および各タグ内の属性情報を取得する。
ステップＳ２８３では、タグ情報および属性情報の解析を行う。
ステップＳ２８４では、画像情報spを分離する。タグおよび属性の情報解析処理をした結果に基づいて画像情報spを抽出する。
ステップＳ２８５では、画像情報spから画像データ形式情報を取り出す。画像情報spの拡張部に格納されている画像データ形式に関する情報または画像部に透かしデータとして埋め込まれている画像データ形式に関する情報を抽出する。タグsp内に画像データ形式が格納されている場合には、このタグsp内の情報を用いることも可能である。
【０１０２】
ステップＳ２８６では、画像データ形式に関する情報に基づいて画像情報spに格納されている各種情報を取り出す。
ステップＳ２８７では、ＯＳ登録画像が利用されているか否かを判別する。ＯＳ登録画像が利用されていると判断した場合にはステップＳ２８８に移行する。
ステップＳ２８８では、ＯＳ登録画像を取得する。たとえば、インターネットなどを介して発行者のサーバにアクセスを行い、ＯＳ登録画像ファイルのダウンロードを行うことでＯＳ登録画像を取得することができる。
【０１０３】
ステップＳ２８９では、処理内容の判別を行う。署名検証の処理を行う場合にはステップＳ２９０に移行し、認証処理を実行する場合にはステップＳ２９１に移行し、利用制御を行う場合にはステップＳ２９２に移行する。
ステップＳ２９０では、画像情報spから抽出した情報とＯＳ登録画像に含まれる情報とを比較して署名情報の検証処理を実行する。
ステップＳ２９１では、画像情報spから抽出した情報と、利用者端末から入力した情報とを比較して、利用者認証処理を実行する。
【０１０４】
ステップＳ２９２では、画像情報spから抽出した情報から文書データの利用制御情報を判別し、利用制限処理を実行する。
〔情報公開システム〕
情報公開システムにおける書類データ管理モデルを、図５１に基づいて説明する。
著作者６０２は自己の著作物である書類および管理情報を管理者６０１に送付し、書類Ａの登録依頼を行う。著作者６０２が管理者６０１に提出する管理情報は、図５２に示すように、書類ごとのアクセスポリシー情報として課金情報を設定することができる。

【０１０５】
管理者６０１は、著作者６０２から登録依頼があった書類を管理者ＤＢ６０５に登録し、登録した書類を公開する。また、管理者６０１は、利用者６０４から公開している書類に対する利用要求を受け付け、著作者６０２が課金要求をしている場合にはこの課金処理を実行する。管理者６０１は課金処理後に著作者６０２が指定する範囲の管理情報を書類に付加し、利用者６０４に送付する。管理者６０１は、書類による利益金を著作者６０２に還元する。
書類に付加される管理情報は、たとえば、図５３のように構成することができる。ここでは、書類表紙６１１に、書類に対して著作者６０２が設定する管理情報表示部６１２、著作者６０２による管理情報が透かしデータとして埋め込まれた画像データ６１３、管理者用の文書管理情報表示部６１４、管理者６０１の管理情報を暗号化して埋め込んだ画像情報６１５などが表示されるようになっている。
【０１０６】
管理者６０１は、図５２に示すように、利用者名、利用日時、利用回数などの利用者ログを生成し、人気ランキングなどの情報を管理情報として管理者ＤＢ６０５に格納する。管理情報中には、利用者６０４から受け付けた所感などの情報を含むように構成でき、必要に応じて著作者６０２にこの情報を送達することもできる。
また、書類の配信を行うプロバイダ６０３は、管理者６０１または著作者６０２の許諾を得て、管理者ＤＢ６０５に格納されている書類の内容公開、著作物の優先公開権利を得る。このプロバイダ６０３は、管理者６０１に代わって書類の配信および課金処理を実行することも可能である。
【０１０７】
（情報公開システムのフローチャート）
この情報公開システムにおける各者の動作を図６８に示す。
著作者は、ステップＳ４０１において、著作者情報などを記録した文書データを作成する。ここでは、自己の著作物に、著作者の個人情報や著作者画像、アクセスポリシーなどの管理情報などを付加した文書データを作成する。
ステップＳ４０２では管理者に対して情報登録要求を行う。
管理者は、ステップＳ４１１において文書構文解析機能をインストールする。
ステップＳ４１２では、著作者からの登録要求に応じて、文書データに管理者情報および著作者画像などを追加する。ここでは、著作者から送られてきたアクセスポリシーなどの管理情報に基づいて、課金情報やアクセスポリシーなどの管理者情報を生成し、これを追加する。
【０１０８】
ステップＳ４１３では、サーバに文書データのタイトル、内容を登録し、これを公開する。
利用者は、ステップＳ４２１において文書構文解析機能のインストールを行う。ステップＳ４２２では、利用者情報の入力を行い、これに基づいてステップＳ４２３において文書データの利用要求を行う。
管理者は、利用者からの文書データの利用要求に基づいて、利用者情報を取得し、利用者認証を行い、アクセスポリシーなどの検証を行う。さらに、文書データ中の特定文書を利用者情報で秘匿し、アクセス制御機能を付加した状態で文書データを作成する。この後、ステップＳ４１６、Ｓ４１７において、文書データの配信と課金要求を行う。
【０１０９】
利用者はステップＳ４２４において、配信された文書データ中の透かしデータにより改竄検出を行い、書類の利用を行う。また、ステップＳ４２５において、課金処理を行う。
管理者は、利用者からの課金処理に基づいてステップＳ４１８において利用料金の還元処理を行う。
また、管理者はステップＳ４１９において、サーバに登録した文書データの情報をプロバイダに送信する。また、ステップＳ４２０において、利用者情報をプロバイダに送信する

。
【０１１０】
プロバイダは、ステップＳ４３１において、管理者から取得した文書データの情報に基づいて、書類の紹介業務を行う。
〔セキュリティ機能の実装〕
インターネットなどの通信機能を通じて文書データを配信する場合における前述したようなセキュリティ機能の実装例を図５４に示す。
管理者側では、ＷＷＷサーバ７０１と、XML構造解析とアクセスを行うインターフェイス７０２、業務アプリケーション７０３とを備えており、種々のデータベース７０４とリンクしている。
【０１１１】
利用者側では、ＷＷＷサーバ７０１から配信される各種データをブラウズ可能なブラウザ７１１と、XML構文解析とアクセスを行うインターフェイス７１２を備えている。
利用者側では、WWWサーバ７０１から送信されるXML文書とXSLスタイルシートとを備える文書データ７２２をブラウザ７１１上で表示し、これに対して入力されたデータをXML文書としてWWWサーバ７０１に返す。
（暗号化と不可視透かし）
画像情報spとして暗号化した秘密情報を埋め込み、閲覧制御を行う場合のタグspの例を図５５に示す。
【０１１２】
図５５に示すようなXML文書の定義を行う場合のフローチャートを図５７に示す。
ステップＳ３０１では、タグの設定を行う。ここでは、セキュリティ処理を定義するための<security>および対象画像を定義するための<mark__file>をタグsp内のタグとして設定している。
ステップＳ３０２では、securityタグ内の認証種別を示す属性authenticateを'password'に設定している。この場合、利用者認証情報をキーボード入力により受け付けるように設定される。
【０１１３】
ステップＳ３０３では、securityタグ内の透かし入り画像データに格納されている情報を定義する属性info__typeの設定を行っている。ここで設定されている属性値'secret'は秘匿情報である旨を示し、属性値'authentication'は、認証情報がmark__fileで指定した画像に格納されていることを示している。
ステップＳ３０４では、securityタグ内の認証処理を示す属性wm__verificationおよび暗号手段を示す属性a__encryptedを定義している。ここで、属性wm__verificationに設定されている'2001.8.30'は認証処理有効期限を示し、属性a__encryptedに設定されている'DES'は、ＤＥＳ暗号により暗号化されていることを示している。
【０１１４】
ステップＳ３０５では、mark__fileタグ内のセキュリティ種別（透かし種別など）を示す属性security__methodおよび透かしデータとして埋め込まれた情報を定義する属性wm__inを定義している。ここで、属性security__methodとして設定されている'invisible__watermark'は、富士通（株）仕様の不可視透かしであることを定義しており、属性wm__inに設定されている't0'は、t0.txtの埋め込みを行ったことを意味している。
なお、図５５のdemo.xml中で定義されるスタイルシートdemo.xslの例を図５６に示す。demo.xmlをブラウザ上で表示する場合、文書中で定義されたスタイルシートの内容に応じて表示される。
【０１１５】
（文書データの生成）
暗号化および不可視の透かしデータを用いた文書データを生成する際のフローチャートを図５８に示す。
ステップＳ３１１では、文書解析処理の定義付けを行う、文書データとなる電子化データ

の内容を登録し、構造化文書を生成するための準備を行う。
ステップＳ３１２では、書類生成アプリを起動する。たとえば、XMLパーサなどを起動して構造化文書の生成を開始する。
【０１１６】
ステップＳ３１３では、秘匿情報、不可視の透かしデータとして埋め込む画像データの指定を行う。
ステップＳ３１４では、認証情報を設定し、透かし関連情報をXML文書に格納する。たとえば、passwordを認証情報として設定し、図５７に示すような手順で、各タグ内の属性値を設定する。
ステップＳ３１５では、秘匿情報を伏せ字化してXML文書に格納する。たとえば、タグsecurityの要素に設定される秘匿情報を'******'にすることで、この要素に記述されたデータを不可視とする。
【０１１７】
ステップＳ３１６では、秘匿情報と認証情報とを不可視の透かしデータにして画像データに埋め込み、画像データ付き文書データを生成する。
（文書データの利用）
暗号化および不可視の透かしデータを用いた文書データを利用する際のフローチャートを図５９に示す。
ステップＳ３２１では、書類利用アプリケーションを起動する。構造化文書を解析するためにXMLパーサなどのアプリケーションを起動し、文書利用の準備を行う。
【０１１８】
ステップＳ３２２では、タグ内の要素および属性を検出する。ここでは、構造化文書の構造を解析し、タグ内に記述されている要素および属性を解析する。
ステップＳ３２３では、タグ内の要素または属性として記述されている認証情報を検出する。
ステップＳ３２４では、画像データに埋め込まれている不可視の透かしデータを抽出してこの透かしデータに含まれている認証情報を検出する。
ステップＳ３２５では、タグ内の要素または属性から検出された認証情報と、画像データ内から抽出された認証情報とを比較し検証する。
【０１１９】
ステップＳ３２６では、タグ内の要素または属性から検出された認証情報と、画像データ内から抽出された認証情報とが一致した場合にはステップＳ３２７に移行し、一致しなかった場合にはステップＳ３２８に移行する。
ステップＳ３２７では、不可視の透かしデータとして画像データ内に埋め込まれている秘匿情報を抽出しこれを表示する。
ステップＳ３２８では、秘匿情報の内容を伏せ字で表示する。
（暗号化、不可視透かし、署名情報）
画像情報spとして暗号化した秘密情報および署名情報を埋め込む場合のタグspの例を図６０に示す。この例では、図５５のdemo.xmlとほぼ同様の構成であり、（４）で示した行が追加された構成となっている。
【０１２０】
この場合の処理のフローチャートを図６１に示す。
ステップＳ３３１において、securityタグ内の透かし入り画像データに格納されている情報を定義する属性info__typeの設定を行っている。ここでは、図５７のステップＳ３０３と同様にして、秘匿情報であることを示す属性値'secret'および認証情報がmark__fileで指定した画像に格納されていることを示す属性値'authentication'を設定するとともに、署名情報がmark__fileで指定した画像に格納されていることを示す属性値'sign'を設定している。
【０１２１】
ステップＳ３３２では、署名範囲を定義するための属性sign__targetの設定を行っている

。ここで、属性sign__targetに設定されている属性値'all'は、署名の対象となる情報がこのXML文書の全要素であることを示している。
ステップＳ３３３では、他のタグ要素を図５５に示すタグ要素と同様に設定する。
（暗号化データおよび署名情報を備える文書データの生成）
暗号化データおよび署名情報を不可視の透かしデータとした文書データを生成する際のフローチャートを図６２に示す。
【０１２２】
ステップＳ３４１では、文書解析処理の定義付けを行う、文書データとなる電子化データの内容を登録し、構造化文書を生成するための準備を行う。
ステップＳ３４２では、書類生成アプリを起動する。たとえば、XMLパーサなどを起動して構造化文書の生成を開始する。
ステップＳ３４３では、図５８のステップＳ３１３～Ｓ３１５と同様の処理を実行する。
ステップＳ３４４は、指定された要素のデジタル署名処理を行う。ここでは、XML文書の全要素についてハッシュ関数などの一方向関数処理を実行し、署名情報を生成する。
【０１２３】
ステップＳ３４５では、署名範囲情報、署名情報を画像データに不可視の透かしデータとして埋め込み、画像データ付き文書データを生成する。
（暗号化データおよび署名情報を備える文書データの利用）
暗号化データおよび署名情報を備える文書データを利用する際のフローチャートを図６３に示す。
ステップＳ３５１では、書類利用アプリケーションを起動する。構造化文書を解析するためにXMLパーサなどのアプリケーションを起動し、文書利用の準備を行う。
【０１２４】
ステップＳ３５２では、タグ内の要素および属性を検出する。ここでは、構造化文書の構造を解析し、タグ内に記述されている要素および属性を解析する。
ステップＳ３５３では、図５９のステップＳ３２３～Ｓ３２８と同様の認証情報による検証処理を行う。
ステップＳ３５４では、文書データのタグsp内で指定されている対象書類の署名情報を生成する。ここでは、指定されている各エレメントのハッシュ値を算出する。
【０１２５】
ステップＳ３５５では、画像データに透かしデータとして埋め込まれている署名情報を抽出する。
ステップＳ３５６では、文書データから生成された署名情報と、透かしデータから抽出された署名情報とを比較して検証処理を行う。
ステップＳ３５７では、文書データから生成された署名情報と、透かしデータから抽出された署名情報とが一致した場合には利用者に文書データを利用させ、一致しなかった場合にはステップＳ３５８に移行する。
【０１２６】
ステップＳ３５８では、エラー処理を実行する。エラー処理は、たとえば、署名情報が一致しなかった旨を表示し利用者に警告を促す、管理者に通知を行うなどの処理が考えられる。
（暗号化および可視透かし）
画像情報spとして可視的な透かしデータを埋め込ん不正利用の防止を行うようにした文書データのタグspの例を図６４に示す。
図６４に示すようなXML文書の定義を行う場合のフローチャートを図６５に示す。
【０１２７】
ステップＳ３６１では、タグの設定を行う。ここでは、セキュリティ処理を定義するための<security>および対象画像を定義するための<mark__file>をタグsp内のタグとして設定している。
ステップＳ３６２では、securityタグ内の可視的な透かしデータの除去情報を定義するた

めの属性wm__removeを設定している。ここで、属性wm__removeの属性値として設定されている'@password'では、可視的な透かしデータ'FJ'の除去情報（password入力した情報を暗号化）を定義している。

【０１２８】

ステップＳ３６３では、securityタグ内のセキュリティ種別を定義する属性security__methodの設定を行っている。ここで設定されている属性値'visible__watermark__f'は富士通（株）仕様の可視的な透かしデータであることを示している。

ステップＳ３６４では、mark__fileタグ内の可視的な透かしデータの情報を定義する属性v__wmを設定している。ここで、属性v__wmとして設定されている'FJ'は、可視的な透かしデータが'FJ'であることを示す。

【０１２９】

ステップＳ３６５では、その他のタグの要素および属性を図５５の文書データと同様に設定している。

（文書データの生成）

暗号化データおよび可視的な透かしデータを用いた文書データを生成する際のフローチャートを図６６に示す。

ステップＳ３７１では、文書解析処理の定義付けを行う、文書データとなる電子化データの内容を登録し、構造化文書を生成するための準備を行う。

【０１３０】

ステップＳ３７２では、書類生成アプリを起動する。たとえば、XMLパーサなどを起動して構造化文書の生成を開始する。

ステップＳ３７３では、可視的な透かしデータおよび埋め込みを行う画像データを指定する。

ステップＳ３７４では、認証情報を設定し、透かし関連情報をXML文書に格納する。たとえば、passwordを認証情報として設定し、図６５に示すような手順で、各タグ内の属性値を設定する。

【０１３１】

ステップＳ３７５では、可視的な透かしデータにして画像データに埋め込み、画像データ付き文書データを生成する。

（文書データの利用）

暗号化データおよび可視的な透かしデータを用いた文書データを利用する際のフローチャートを図６７に示す。

ステップＳ３８１では、書類利用アプリケーションを起動する。構造化文書を解析するためにXMLパーサなどのアプリケーションを起動し、文書利用の準備を行う。

【０１３２】

ステップＳ３８２では、タグ内の要素および属性を検出する。ここでは、構造化文書の構造を解析し、タグ内に記述されている要素および属性を解析する。

ステップＳ３８３では、タグ内の要素または属性として記述されている認証情報を検出する。

ステップＳ３８４では、利用者が入力する認証情報を受け付ける。

ステップＳ３８５では、タグ内の要素または属性から検出された認証情報と、入力された認証情報とを比較し検証する。

【０１３３】

ステップＳ３８６では、タグ内の要素または属性から検出された認証情報と、入力された認証情報とが一致した場合にはステップＳ３８７に移行し、一致しなかった場合にはステップＳ３８８に移行する。

ステップＳ３８７では、可視的な透かしデータを除去して画像データの表示を行う。

ステップＳ３８８では、可視的な透かしデータが埋め込まれた情報で画像データの表示を行う。

【０１３４】

（書類の利用制御）
権利保護を目的とした文書利用の制御を行う場合の例を図７０に示す。
管理者側におけるサーバ９００には、複数の書類９０１が管理されているデータベースが構築されている。この書類９０１はそれぞれ構造化文書（XML文書）９０２、スタイルシート（XSL文書）９０３および秘匿情報を電子透かしとして備える画像データ９０４とを含んでいる。
利用者側のユーザコンピュータ９５０では、管理者側のサーバ９００で管理されている書類９０１を利用するためのアプリケーションソフトがインストールされており、このアプリケーションを用いて書類検索・ダウンロードおよび書類の利用を行う。
【０１３５】
ユーザコンピュータ９５０では、サーバ９００のデータベース内の書類を利用するために、利用者登録機関９２０に利用者登録を行う。ここでは、利用者の個人情報などを利用者登録機関９２０に送信し、利用者登録機関９２０から管理者のサーバ９００に利用者情報の通知を送信する。
ユーザコンピュータ９５０では、インターネット網や公衆回線網、その他のネットワークを通じて管理者側のサーバ９００にアクセスを行い、書類の検索処理を行う。この場合、たとえば、既存のサーチエンジンなどを用いて検索することが可能であり、サーバ９００で用意されているサーチエンジンにより検索するように構成することも可能である。
【０１３６】
ユーザコンピュータ９５０から通知されるカテゴリー、キーワードなどに基づいて検索された結果は、サーバ９００からユーザコンピュータ９５０に通知される。この検索結果通知は、ユーザコンピュータ９５０のブラウザなどにより利用者に認識できるように表示される。
ユーザコンピュータ９５０側において表示された検索結果通知のうち、利用者が利用を希望する書類が選択されると、そのファイル指定情報がサーバ９００に送信される。
【０１３７】
サーバ９００は、ユーザコンピュータ９５０から送信されてくるファイル指定情報に基づいて、利用者登録機関９２０から通知された利用者情報に基づいて利用者に対応する画像データ９０４を生成し、書類９０１をユーザコンピュータ９５０に送信する。
ユーザコンピュータ９５０では、パスワードやその他の利用者認証情報を入力させて認証処理を行う。認証処理の結果、利用者の認証が正常に行うことができなかった場合には、秘匿情報部分についてはアスタリスクなどによる伏せ字表示とする。
【０１３８】
また、利用者の認証を正常に行うことができた場合には、秘匿情報を取得する。たとえば、画像データ９０４内に電子透かしとして埋め込まれた秘匿情報を取り出して、暗号化されている場合には復号化を行う。
秘匿情報を正常に取得することができた場合には、文書データと合成して秘匿情報の表示を行う。
たとえば、図７１に示すように、サーバ９００で管理しているデータベース内の構造化書類９０２が、電子透かしの復元情報９０５と、不可視の電子透かしとして埋め込まれた原情報の存在場所を示す格納情報９０６とを含む構成である場合を考察する。
【０１３９】
この場合、利用者側からのファイル指定情報に基づいてユーザコンピュータ９５０に送信される書類９０１には、構造化文書９０２と、スタイルシート９０３および秘匿情報が電子透かしとして埋め込まれた画像データ９０４とを含んでいる。ユーザコンピュータ９５０では、電子透かしとして秘匿情報の原情報を含む画像データを表示するための画像表示部９７２および伏せ字または秘匿情報の原情報を表示する秘匿情報表示部９７１とを含む表示用文書９７０が表示されることとなる。
【０１４０】
利用者の認証に失敗した場合には、表示用文書９７０の秘匿情報表示部９７１には、図７

２に示すように、伏せ字表示９７３が表示される。また、利用者の認証に成功した場合には、表示用文書９７０の秘匿情報表示部９７１には、図７３に示すように、原情報９７４が表示される。
このように構成した場合、正当な利用者に対してのみ、秘匿情報の原情報を表示するように構成でき、著作権者や文書の頒布権を有する者の権利保護をはかることが可能となる。また、利用者側のユーザコンピュータ９５０にダウンロードを行った後であっても、文書利用を行う毎に利用者認証を行うように構成できるため、不正利用を行うことが困難となり、著作権者や頒布権者の利益を損なうことを低減できる。
【０１４１】
〔印刷物からの利用制御情報取得〕
利用制御情報が不可視透かしとして埋め込まれた画像をデジタルカメラやイメージスキャナなどで電子化データとして取り込んで、データを利用するためのデータ管理装置について説明する。
図７４はデータ管理装置の簡略構成を示す機能ブロック図である。
このデータ管理装置は、電子化データを取得するための画像入力部１００１と、画像入力部１００１から取り込まれた電子化データを解析して利用制御情報を抽出する画像解析部１００２と、画像解析部１００２で抽出された利用制御情報に対応するテキストデータ、画像データ、音楽データ、その他の電子化データで構成される文書データを取得する情報管理部１００３と、情報管理部１００３で取得した文書データに基づいて構造化文書を生成するXML文書生成部１００４とを含んでいる。
【０１４２】
画像入力部１００１は、利用制御情報が不可視透かしとして埋め込まれた画像がデジタルカメラやイメージスキャナなどにより変換された電子化データを取得するものである。
画像解析部１００２は、画像入力部１００１で取得した電子化データから情報要素を取り出して利用制御情報を抽出するものであり、たとえば、図７５に示すような手順で各電子データの解析処理を実行する。
まず、取得した電子化データを要素分離機能部１０２１により絵や写真などの画像データ１０２２と、透かしを抽出するための制御情報を含むテキストデータ１０２３とに要素分離処理を実行する。
【０１４３】
分離されたテキストデータ１０２３は、テキスト解析機能部１０２４により解析されて透かしを抽出するための制御情報１０２５が抽出される。テキスト情報１０２３は、構造化文書を生成するためにXML文書化機能部１０２６によりXML文書化される。
透かし抽出機能部１０２７は、テキストデータ１０２３より抽出された透かし抽出制御情報１０２５を用いて画像データ１０２２から透かし情報１０２８を抽出する。
【０１４４】
画像データ１０２２から抽出された透かし情報１０２８は、透かし情報解析機能部１０２９により解析される。透かし情報１０２８は、データの利用制限やリンク先となるウェブサイトのアドレス情報、その他の利用制御情報を含んでいる。
情報管理部１００３では、透かし情報１０２８中の利用制御情報に基づいて、これに対応するテキストデータ、画像データ、音楽データ、その他の電子化データで構成される文書データを取得するものであり、たとえば図７６に示すような手順でデータ処理を実行する。
【０１４５】
利用情報解析機能部１０３１では、画像解析部１００２で抽出された利用制御情報に基づいて、対応するテキストデータ、画像データ、音楽データ、その他の電子化データで構成される文書データを取得する。
たとえば、利用制御情報中に利用制限に関するデータが含まれている場合には、ユーザの認証を行って、その認証結果に基づいて利用制限を行うように構成することが可能である。

また、利用制限情報中にリンク先となるウェブサイトのアドレス情報が含まれているような場合には、該当するウェブサイトへのアクセスを実行し、そこに含まれるテキストデータ、画像データ、音楽データなどの文書データを取得する。

【０１４６】

XMLデータ生成機能部１０３２では、利用情報解析機能部１０３１で取得した文書データに対してTAGや属性値を設定し、構造化文書のデータを生成する。ウェブサイトから取得した各文書データについては、そのフォーム番号を参照して、TAGや属性値表を作成し、属性値データベース１０３４に格納する。

リンク指定機能部１０３３では、ウェブサイトなどから取得した文書データ中にさらにリンク情報が付加されている場合に、そのリンク情報を取得して構造化文書のデータとするとともに、リンク情報データベース１０３５にこのデータを格納する。

【０１４７】

XML文書生成部１００４では、情報管理部１００３で生成されたXMLデータに基づいて、XML文書を生成するものである。情報管理部１００３で生成されたXMLデータが、たとえば、図７７に示すような、画像データで構成される情報１、テキストデータで構成される情報２および情報３の情報要素を含む場合、図右に示すような構造化文書を生成することとなる。

利用制御情報を不可視透かしとして埋め込まれた画像データを生成するための処理フローを図７８に示す。

【０１４８】

ステップＳ４０１では、出力される画像データの元となる画像データやテキストデータなどの入力を受け付ける。

ステップＳ４０２では、ステップＳ４０１で受け付けた各データの構造化処理を実行する。ここでは、各データの配置や構成を決定し、出力される画像データの構造を決定する。このとき、ステップＳ４０３において、利用制御情報を生成し、これを画像データ中に不可視透かしとして埋め込むための処理を実行する。

ステップＳ４０４では、不可視透かしとして画像データ中に埋め込まれた利用制御情報を抽出するための透かし抽出用制御情報を生成する。ここでは、透かし情報が画像データのどの位置に埋め込まれているかを示す位置情報、透かしの種別情報、透かしのバージョン情報などを透かし抽出用制御情報として生成する。

【０１４９】

ステップＳ４０５では、構造化された各データと生成された透かし抽出用制御情報とに基づいて画像データを合成し最終的な画像データを出力する。

このようにして生成される画像データは、たとえば、プリンタなどを用いて紙に印刷されるなどして印刷物として配布される。配布された印刷物上の画像データは、デジタルカメラやイメージスキャナなどにより電子化データとして取り込んで、利用制御情報に対応する各種データを利用することが可能となる。データ利用時における文書管理装置の処理フローを図７９に示す。

【０１５０】

ステップＳ４１１では、画像入力部１００１により画像データを取得する。前述したように、印刷物として配布された画像データをデジタルカメラやイメージスキャナなどによって電子化データとして取り込み、この電子化データを画像入力部１００１によって取得するように構成できる。

ステップＳ４１２では、画像解析部１００２の要素分離機能部１０２１により、画像データ１０２２とテキストデータ１０２３に分離する。

ステップＳ４１３では、分離された画像データ１０２２およびテキストデータ１０２３の解析処理を実行する。ここでは、テキスト解析機能部１０２４によりテキストデータ１０２３を解析し、透かし抽出用の制御情報を抽出する。

【０１５１】

ステップＳ４１４では、抽出された透かし抽出用の制御情報に基づいて、画像データ中に

埋め込まれた不可視透かしを抽出し、利用制御情報を取得する。
ステップＳ４１５では、利用制御情報に対応する各種データを取得し、これに基づいてXML構造化文書を生成する。
この実施形態において、構造化文書としてXML文書を採用したが、HTMLやその他の構造化文書を採用することが可能である。
＜付記＞
（付記１）
テキストデータ、画像データ、音楽データ、その他の電子化データで構成される文書データに対して複数の情報項目毎に識別子を設定し、前記識別子内に前記情報項目毎の内容情報を格納する構造化文書の配布方法であって、
（Ａ）前記文書データを利用するために必要となる利用制御情報を生成し、前記利用制御情報を相補的に構成する第１利用制御情報と第２利用制御情報とに分離する段階と、
（Ｂ）特定のデータを管理情報格納用データとして指定し、前記第１利用制御情報を前記管理情報格納用データ内に埋め込む段階と、
（Ｃ）前記第１利用制御情報が埋め込まれた管理情報格納用データを前記文書データ内の情報項目とするための管理用識別子を設定する段階と、
（Ｄ）前記管理用識別子内に、前記第１利用制御情報が埋め込まれた管理情報格納用データの内容情報と、前記管理情報格納用データから第１利用制御情報を抽出し前記第１利用制御情報とともに文書データを利用するための利用制御情報を生成する第２利用制御情報とを格納する段階と、
を含む文書配布方法。
【０１５２】
（付記２）
前記管理情報格納用データは画像データまたは音楽データなどの電子化データを含み、前記Ｂの段階において、前記第１利用制御情報を視覚的または聴覚的に認識不能な透かしデータとして前記管理情報格納用データ内に埋め込むことを特徴とする、付記１に記載の文書配布方法。
（付記３）
前記管理情報格納用データは画像データまたは音楽データなどの電子化データを含み、前記Ｂの段階において、前記第１利用制御情報を視覚的または聴覚的に認識可能なデータとして前記管理情報格納用データ内に格納することを特徴とする、付記１に記載の文書配布方法。
【０１５３】
（付記４）
前記管理情報格納用データは画像データまたは音楽データなどの電子化データでなる第１データ部と第２データ部とを備え、前記Ｂの段階において、前記第１利用制御情報を暗号化した暗号化利用制御情報を生成し、前記暗号化利用制御情報を前記第２データ部に格納するとともに、前記暗号化利用制御情報を生成した際の暗号鍵情報を視覚的または聴覚的に認識不能な透かしデータとして前記第１データ部に埋め込むことを特徴とする、付記１に記載の文書配布方法。
【０１５４】
（付記５）
前記第２利用制御情報は、前記文書データの改竄防止範囲を指定する範囲指定情報、前記透かしデータが埋め込まれた電子化データのデータ種別情報、前記第１利用制御情報の情報種別を示す制御種別情報、前記文書データに含まれる電子化データに対するアクセスポリシー情報、前記第１利用制御情報を透かしデータに変換する際の透かし制御情報、前記第１利用制御情報のデータ名のうち少なくとも１つを含む、付記１～４のいずれかに記載の文書配布方法。
【０１５５】
（付記６）

前記第１利用制御情報は、画像データ、音楽データ、暗号／認証／署名関連データ、制御プログラムのうちの少なくとも１つを含む画像データまたは音楽データのファイルフォーマットで構成される、付記１～５のいずれかに記載の文書配布方法。
（付記７）
前記管理用識別子内に格納される情報内容を複製して複製情報を生成し、前記複製情報を電子透かしとして前記管理情報格納用データ内に埋め込む段階をさらに含む、付記１～６のいずれかに記載の文書配布方法。
【０１５６】
（付記８）
前記文書データ内の電子化データのうち所定範囲に含まれる電子化データを秘匿情報として抽出し、前記秘匿情報を他の表示用情報と置き換えた電子化データを前記管理情報格納用データとし、前記秘匿情報を前記管理情報格納用データ内に格納する、付記１～７のいずれかに記載の文書配布方法。
（付記９）
前記秘匿情報を視覚または聴覚を通じて認識不能な透かしデータとして前記管理情報格納用データ内に埋め込むことを特徴とする、付記８に記載の文書配布方法。
【０１５７】
（付記１０）
前記秘匿情報を暗号化して前記管理情報格納用データ内に格納することを特徴とする、付記８に記載の文書配布方法。
（付記１１）
前記文書データ内の電子化データのうち所定範囲に含まれる電子化データの署名値を算出し、前記署名値を前記管理情報格納用データ内に格納することを特徴とする、付記１～１０のいずれかに記載の文書配布方法。
【０１５８】
（付記１２）
テキストデータ、画像データ、音楽データ、その他の電子化データで構成される文書データに対して複数の情報項目毎に識別子を設定し、前記識別子内に前記情報項目毎の内容情報を格納する構造化文書のデータ生成装置であって、
前記文書データを利用するために必要となる利用制御情報を生成する利用制御情報生成手段と、
特定のデータを管理情報格納用データとして指定し、前記利用制御情報の一部を構成する第１利用制御情報を前記管理情報格納用データ内に格納する第１管理情報格納手段と、
前記文書データに含まれる電子化データを情報項目毎に識別子を設定し、前記識別子内に前記情報項目毎の内容情報を格納する文書構造生成手段と、
前記管理情報格納用データを前記文書データ内の情報項目とするための管理用識別子を設定し、前記第１利用制御情報とともに相補的に前記利用制御情報を構成する第２利用制御情報を前記管理用識別子の内容情報として格納する第２管理情報格納手段と、
を備える文書データ生成装置。
【０１５９】
（付記１３）
テキストデータ、画像データ、音楽データ、その他の電子化データで構成される文書データに対して複数の情報項目毎に識別子を設定し、前記識別子内に前記情報項目毎の内容情報を格納する構造化文書のデータ利用装置であって、
配布される文書データの文書構造を解析する文書構造解析手段と、
前記文書データに含まれる管理用識別子内の第２利用制御情報を抽出する第２利用制御情報抽出手段と、
前記第２利用制御情報と、前記文書データに含まれる管理情報格納用データ内の第１利用制御情報とに基づいて、前記文書データを利用させる文書データ利用手段と、
を備える文書データ利用装置。

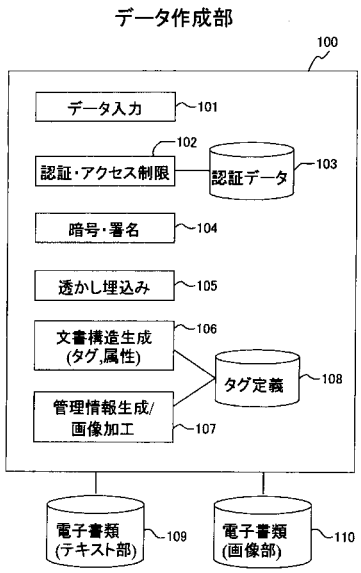
【０１６０】
（付記１４）
テキストデータ、画像データ、音楽データ、その他の電子化データで構成される文書データに対して複数の情報項目毎に識別子を設定し、前記識別子内に前記情報項目毎の内容情報を格納する構造化文書の配布方法をコンピュータに実行させるプログラムであって、
（Ａ）前記文書データを利用するために必要となる利用制御情報を生成し、前記利用制御情報を相補的に構成する第１利用制御情報と第２利用制御情報とに分離する段階と、
（Ｂ）特定のデータを管理情報格納用データとして指定し、前記第１利用制御情報を前記管理情報格納用データ内に埋め込む段階と、
（Ｃ）前記第１利用制御情報が埋め込まれた管理情報格納用データを前記文書データ内の情報項目とするための管理用識別子を設定する段階と、
（Ｄ）前記管理用識別子内に、前記第１利用制御情報が埋め込まれた管理情報格納用データの内容情報と、前記管理情報格納用データから第１利用制御情報を抽出し前記第１利用制御情報とともに文書データを利用するための利用制御情報を生成する第２利用制御情報とを格納する段階と、
を含む文書配布方法のプログラム。
【０１６１】
（付記１５）
（Ａ）視覚的または聴覚的に認識不能な透かしデータとして利用制御情報が埋め込まれた情報を電子化データとして取得する段階と、
（Ｂ）前記電子化データから前記利用制御情報を抽出する段階と、
（Ｃ）前記利用制御情報に対応する特定のテキストデータ、画像データ、音楽データ、その他の電子化データで構成される文書データの書類情報を取得する段階と、
（Ｄ）前記書類情報に対して複数の情報項目毎に識別子を設定し、前記識別子内に情報項目毎の内容情報を格納する構造化文書を生成する段階と、
を含む文書管理方法。
【０１６２】
（付記１６）
視覚的に認識不能な不可視透かしとして利用制御情報が埋め込まれた画像から電子化画像データに変換する、付記１５に記載の文書管理方法。
（付記１７）
利用制御情報はインターネットでアクセス可能なウェブサイト上のリンクアドレスである、付記１５または１６に記載の文書管理方法。
（付記１８）
視覚的または聴覚的に認識不能な透かしデータとして利用制御情報が埋め込まれた情報を電子化データとして取得するデータ取得手段と、
前記データ取得手段により取得した電子化データから利用制御情報を抽出する利用制御情報抽出手段と、
前記利用制御情報抽出手段により抽出した利用制御情報に対応する特定のテキストデータ、画像データ、音楽データ、その他の電子化データで構成される文書データの書類情報を取得する書類情報取得手段と、
前記書類情報取得手段により取得した書類情報に対して複数の情報項目毎に識別子を設定し、前記識別子内に情報項目毎の内容情報を格納する構造化文書を生成する構造化文書生成手段と、
を備える文書管理装置。
【０１６３】
（付記１９）
前記データ取得手段は、視覚的に認識不能な不可視透かしとして利用制御情報が埋め込まれた画像をデジタルカメラまたはイメージスキャナにより変換された電子化データを取得する、付記１８に記載の文書管理装置。

（付記２０）
前記利用制御情報は、インターネットでアクセス可能なウェブサイト上のリンクアドレスである、付記１８または１９に記載の文書管理装置。
【０１６４】
（付記２１）
（Ａ）視覚的または聴覚的に認識不能な透かしデータとして利用制御情報が埋め込まれた情報を電子化データとして取得する段階と、
（Ｂ）前記電子化データから前記利用制御情報を抽出する段階と、
（Ｃ）前記利用制御情報に対応する特定のテキストデータ、画像データ、音楽データ、その他の電子化データで構成される文書データの書類情報を取得する段階と、
（Ｄ）前記書類情報に対して複数の情報項目毎に識別子を設定し、前記識別子内に情報項目毎の内容情報を格納する構造化文書を生成する段階と、
を含む文書管理方法をコンピュータに実行させるプログラム。
【０１６５】
【発明の効果】
本発明では、文書データを利用するために必要となる利用制御情報を相補的な第１利用制御情報と第２利用制御情報とに分離して、一方を電子化データ内に埋め込み、他方を構造化文書内に格納しているため、改竄検出、真正性の保証、アクセスポリシーや利用者認証などのアクセス制御を確実に行うことが可能となる。
【図面の簡単な説明】
【図１】データ作成装置の機能ブロック図。
【図２】データ利用装置の機能ブロック図。
【図３】構造化文書の説明図。
【図４】タグspの構造を示す説明図。
【図５】タグspの構造を示す説明図。
【図６】タグspの要素として格納される情報種別を示す説明図。
【図７】タグspの属性として格納される情報種別を示す説明図。
【図８】タグspの要素または属性として格納されるデータ書式の説明図。
【図９】画像情報spのデータ形式を示す説明図。
【図１０】文書データ生成のフローチャート。
【図１１】文書データ利用のフローチャート。
【図１２】文書データ生成のフローチャート。
【図１３】文書データ利用のフローチャート。
【図１４】文書タグ生成のフローチャート。
【図１５】文書タグ利用のフローチャート。
【図１６】文書タグ生成のフローチャート。
【図１７】文書タグ利用のフローチャート。
【図１８】アクセスポリシーの種別を示す説明図。
【図１９】文書タグ生成のフローチャート。
【図２０】文書タグ利用のフローチャート。
【図２１】経路情報の種別を示すフローチャート。
【図２２】文書データ生成のフローチャート。
【図２３】文書データ利用のフローチャート。
【図２４】文書データ生成のフローチャート。
【図２５】文書データ利用のフローチャート。
【図２６】暗号化画像として用いられる画像データの種別を示す説明図。
【図２７】暗号化画像生成・利用の説明図。
【図２８】文書データ生成のフローチャート。
【図２９】文書データ利用のフローチャート。
【図３０】画像情報spのデータ格納のフローチャート。

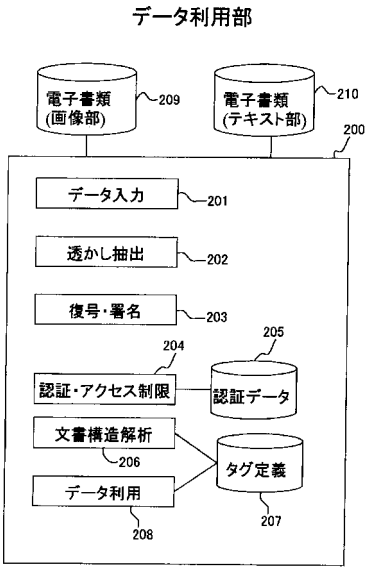
【図３１】画像情報spのデータ格納のフローチャート。
【図３２】画像情報spのデータ格納のフローチャート。
【図３３】画像情報spのデータ格納のフローチャート。
【図３４】画像情報spのデータ変換のフローチャート。
【図３５】画像情報spの復号処理のフローチャート。
【図３６】秘匿情報検証時のフローチャート。
【図３７】秘匿情報検証時のフローチャート。
【図３８】署名情報検証時のフローチャート。
【図３９】署名情報検証時のフローチャート。
【図４０】画像情報spに格納されるデータの情報種別を示す説明図。
【図４１】画像情報spの表示画像を示す説明図。
【図４２】ＯＳ登録画像の登録時におけるフローチャート。
【図４３】ＯＳ登録画像の利用時におけるフローチャート。
【図４４】ＯＳ登録画像を用いた情報管理の制御ブロック図。
【図４５】文書データ生成のフローチャート。
【図４６】文書データの構造を示す説明図。
【図４７】画像情報spに格納される画像データの形式を示す説明図。
【図４８】文書データ利用のフローチャート。
【図４９】紙書類の電子化管理処理を示す説明図。
【図５０】電子書類の管理処理を示す説明図。
【図５１】情報公開システムの説明図。
【図５２】情報公開システムに用いられる管理情報を示す説明図。
【図５３】管理情報が埋め込まれた文書データの一例を示す説明図。
【図５４】セキュリティ機能の実装例を示す説明図。
【図５５】　XML文書に記述されるタグspの一例を示す説明図。
【図５６】　XSLスタイルシートの一例を示す説明図。
【図５７】文書型定義のフローチャート。
【図５８】文書データ生成のフローチャート。
【図５９】文書データ利用のフローチャート。
【図６０】　XML文書に記述されるタグspの一例を示す説明図。
【図６１】文書型定義のフローチャート。
【図６２】文書データ生成のフローチャート。
【図６３】文書データ利用のフローチャート。
【図６４】　XML文書に記述されるタグspの一例を示す説明図。
【図６５】文書型定義のフローチャート。
【図６６】文書データ生成のフローチャート。
【図６７】文書データ利用のフローチャート。
【図６８】情報公開システムのフローチャート。
【図６９】電子化文書の認証情報を紙書類に反映する例の説明図。
【図７０】書類の利用制御を行う例の説明図。
【図７１】　XML文書のセキュリティ例の説明図。
【図７２】利用者認証の結果に基づく表示例の説明図。
【図７３】利用者認証の結果に基づく表示例の説明図。
【図７４】透かしデータが埋め込まれた印刷物などからデータの利用を行う文書管理装置の概略構成を示す機能ブロック図。
【図７５】画像解析部の機能ブロック図。
【図７６】情報管理部の機能ブロック図。
【図７７】生成されるXML文書の構成例を示す説明図。
【図７８】透かしデータが埋め込まれた印刷物などのデータの生成処理を示すフローチャート。

【図７９】透かしデータが埋め込まれた印刷物からXML文書を生成する処理を示すフローチャート。

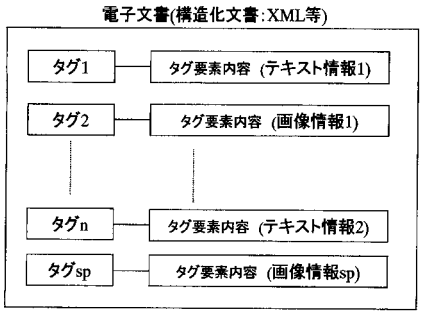
【図１】



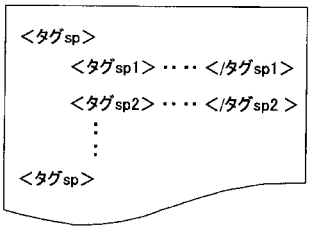
【図２】



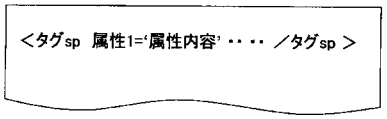
【図３】



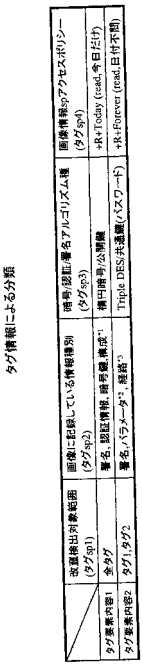
【図４】



【図５】



【図６】



タグ情報による分類

	改竄検出対象範囲 (タグsp1)	画像に記録している情報種別 (タグsp2)	暗号/認証/署名アルゴリズム種 (タグsp3)	画像情報spアクセスポリシー (タグsp4)
タグ要素内容1	全タグ	署名, 認証情報, 暗号鍵, 構成*1,	楕円暗号/公開鍵	+R+Today (read,今日だけ)
タグ要素内容2	タグ1,タグ2	署名, パラメータ*2, 履歴*3	Triple DES/共通鍵(パスワード)	+R+Forever (read,日付不問)

【図７】

属性情報による分類

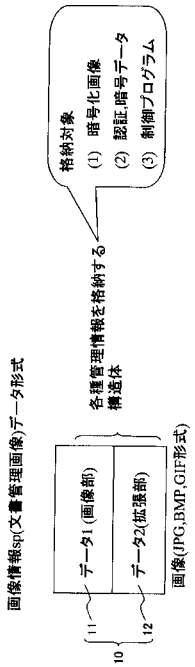
	改竄検出対象範囲 (属性1)	画像に記録している情報種別 (属性2)	暗号/認証/署名アルゴリズム種別 (属性3)	画像情報spアクセスポリシー (属性4)
属性内容1	全タグ	署名, 認証情報, 暗号鍵	楕円暗号/公開鍵	+R+Today (read,今日だけ)
属性内容2	TAG1,TAG2	署名	Triple DES/共通鍵(パスワード)	+R+Forever (read,日付不問)

【図８】

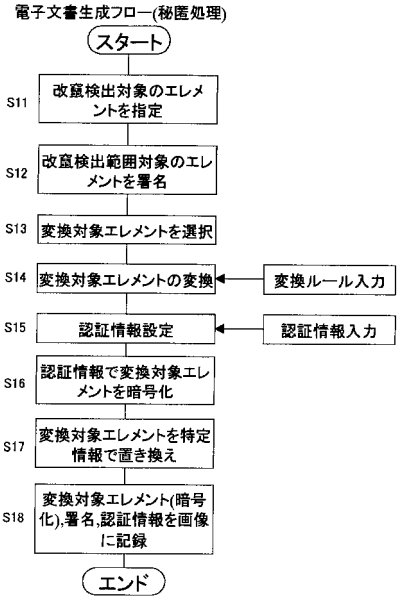
タグ,属性名による書式

タグ,属性名	機能	記述例 <タグ名> 属性=属性値
透かし制御	透かし処理に関するパラメータ	<透かし制御>属性=EMBED </透かし制御> (透かし埋め込み)
透かし制御	透かし処理に関するパラメータ	<透かし制御>属性=1-S0 </透かし制御> (透かし種別1:攻撃耐性強モード)
不可視情報埋め込みデータ名	透かし埋め込み/抽出対象ファイル名	<透かし対象名> Content1.jpg </透かし対象名>
パラメータ*2	格納物(制御プログラム)の動作条件	</パラメータ> プログラム 属性=a </パラメータ>
パラメータ*2	格納物(暗号化画像)の指定	</パラメータ> 画像 </パラメータ>
構成*1	データ格納種別	<構成> データ格納(1) </構成> *データ形式による書式(別表記例) <タグ1> 構成 属性=データ格納(1) </タグ1>

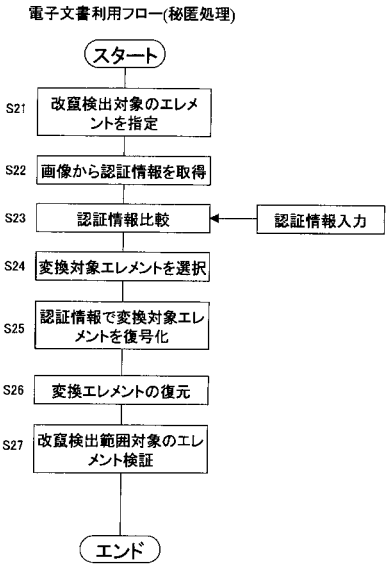
【図９】



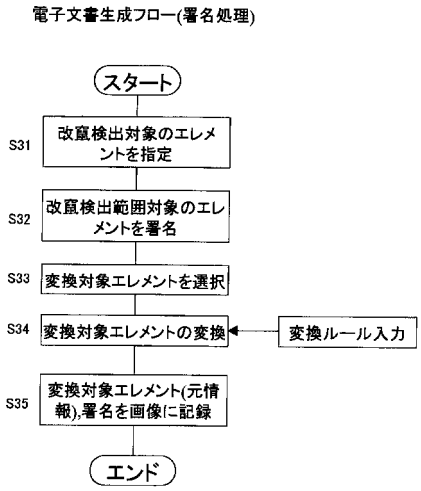
【図１０】



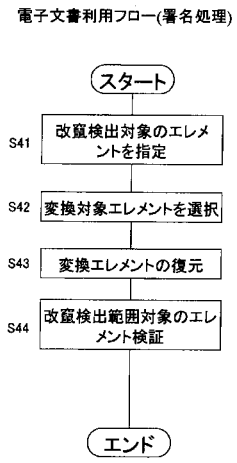
【図１１】



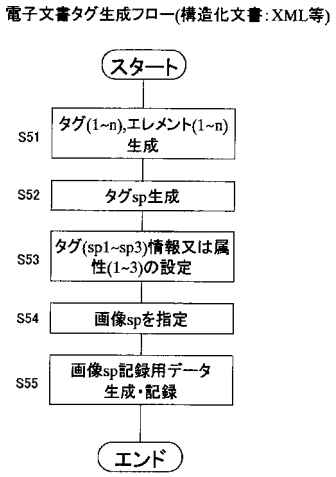
【図１２】



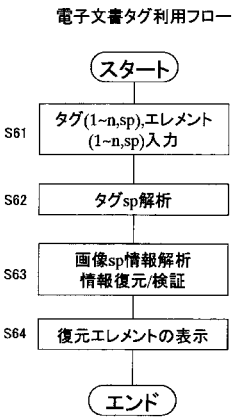
【図１３】



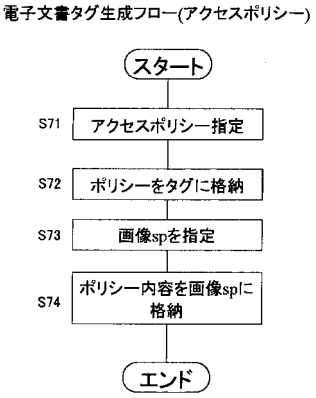
【図１４】



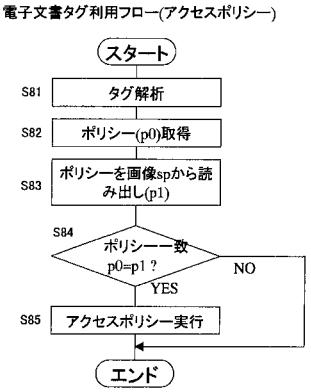
【図１５】



【図１６】



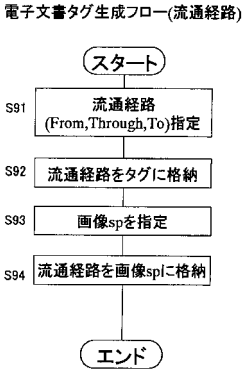
【図１７】



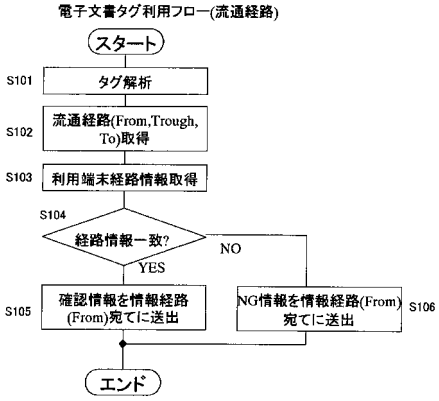
【図１８】

有効期限	残利用回数	利用者属性	処理権限
~YY.MM.DD	カウントダウン	個人利用(+S)	読むだけ(+R)
~Forever		グループ利用(+G)	書き換え可能(+W)
Today(今日だけ)			追記可能(+A)

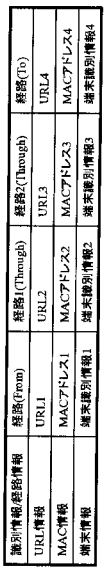
【図１９】



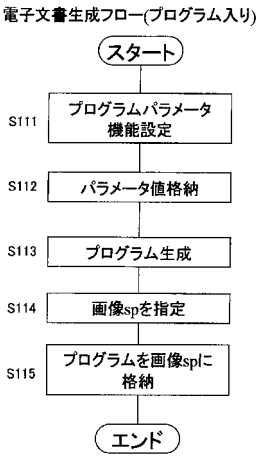
【図２０】



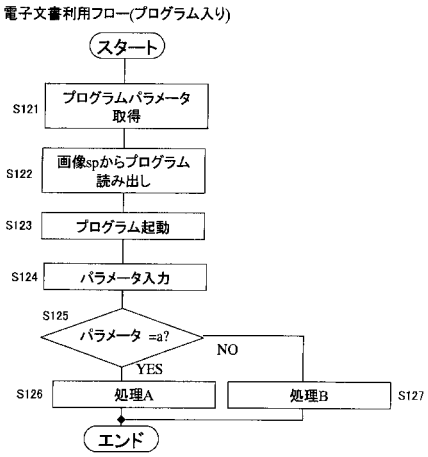
【図２１】



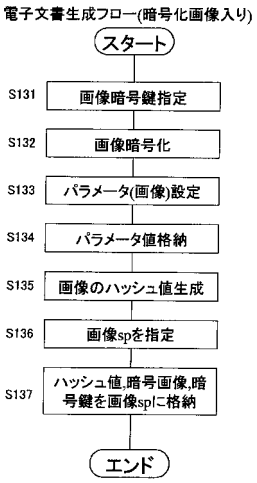
【図２２】



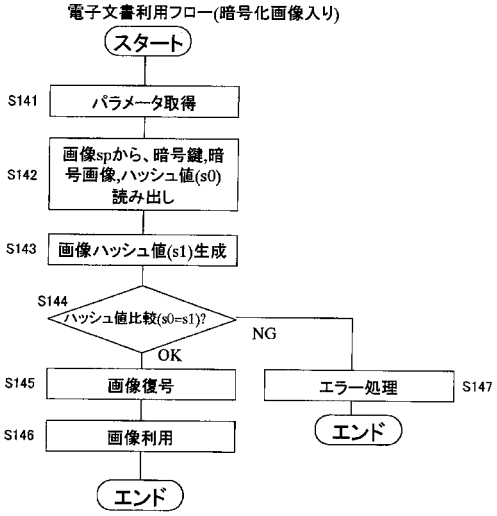
【図２３】



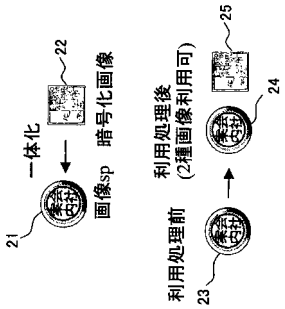
【図２４】



【図２５】



【図２７】

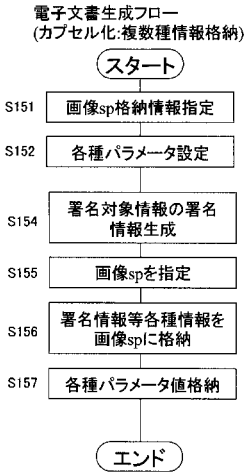


【図２６】

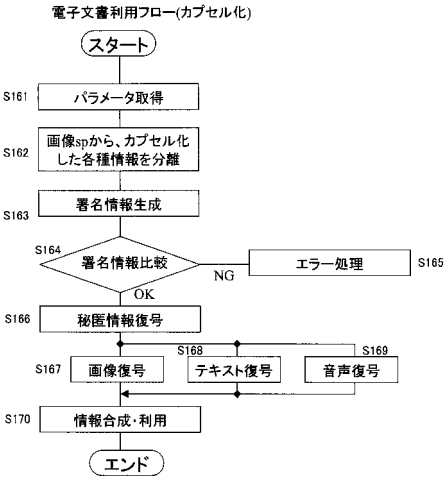
画像内容

顔部(写真,イラスト)画像	視覚的な認証
サイン,署名(画像化)	視覚的な認証
指紋画像	

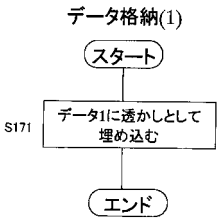
【図２８】



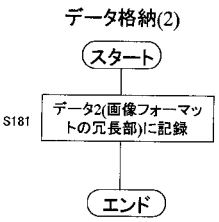
【図２９】



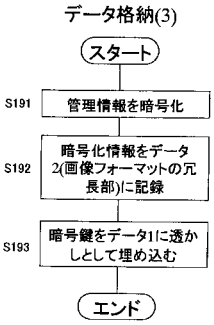
【図３０】



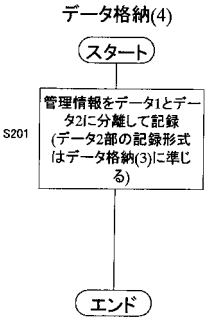
【図３１】



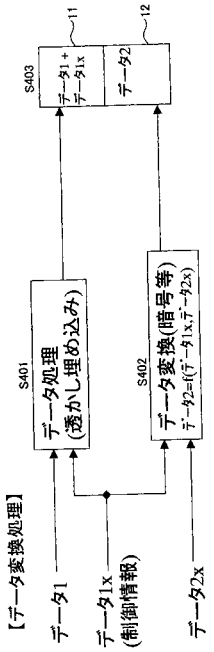
【図３２】



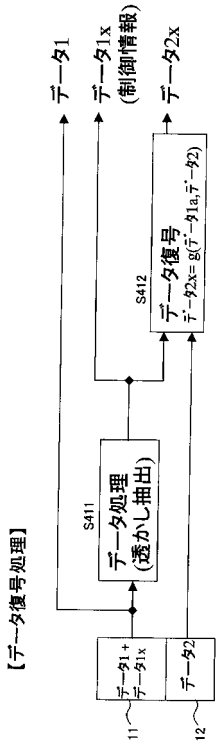
【図３３】



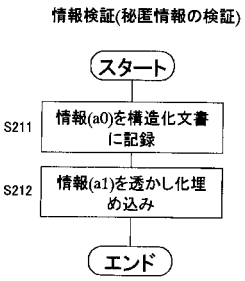
【図３４】



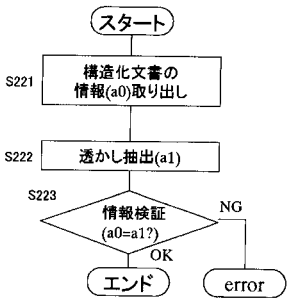
【図３５】



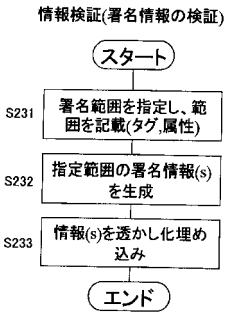
【図３６】



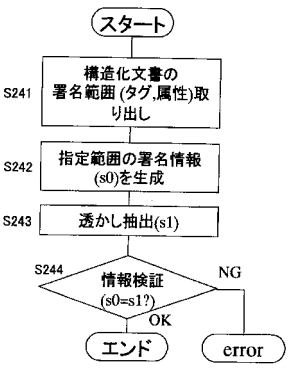
【図３７】



【図３８】



【図３９】

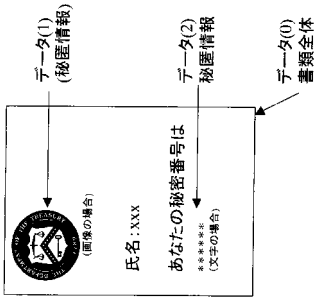


【図４０】

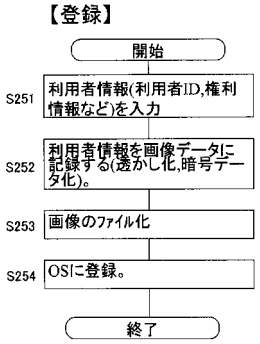
画像情報spデータ拡張部形式
(又は、透かし埋め込みデータ)

データ形式	種別情報
データ(0)全体の特徴情報	署名(Hash値), timestamp
データ(1)の特徴情報	署名(Hash値), timestamp
データ(1)のアクセスポリシー	利用者名,期間,読み書き
データ(2)の特徴情報	署名(Hash値), 部分文字,timestamp
データ(2)のアクセスポリシー	利用者名,期間,読み書き 権利者ID,連絡先,URL, 利用期限,利用許可回数
プログラム	JAVAプログラムなど

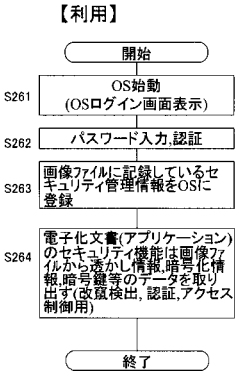
【図４１】



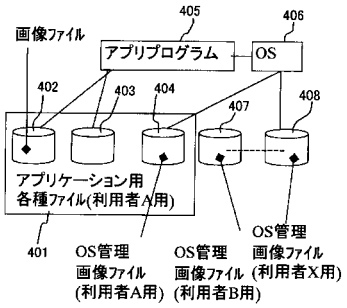
【図４２】



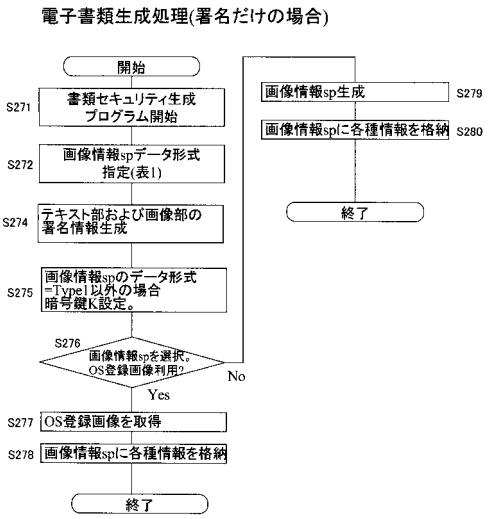
【図４３】



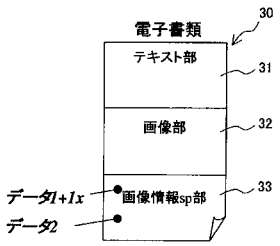
【図４４】



【図４５】



【図４６】



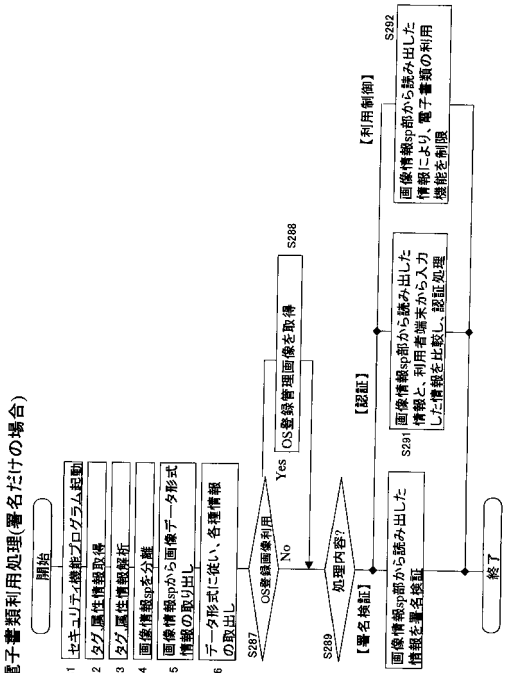
【図４７】

画像データ形式

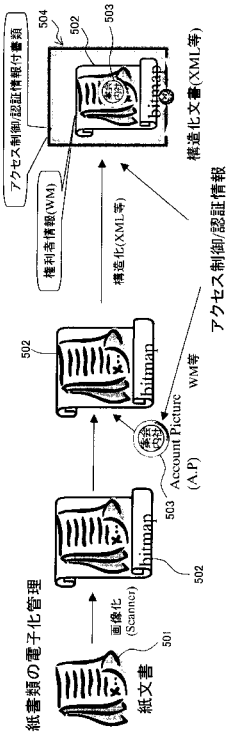
Type1	署名情報を透かし化 (データ1X)
Type2	署名情報,暗号鍵を透かし化(データ1X) 署名/暗号化対象情報データを拡張部に記録(データ2X)
Type3	署名情報を透かしデータ化(データ1X) 暗号鍵,署名/暗号化対象情報データをデータ拡張部に記録(データ2X)
Type4	暗号鍵を透かし化(データ1X) 署名情報,署名/暗号化対象情報データをデータ拡張部に記録 (データ2X)

入力データ(テキスト部・画像部の署名情報, テキスト部の暗号鍵,署名/暗号範囲)

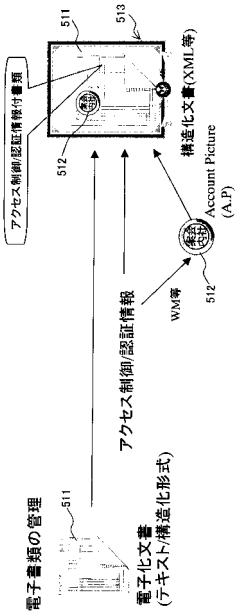
【図４８】



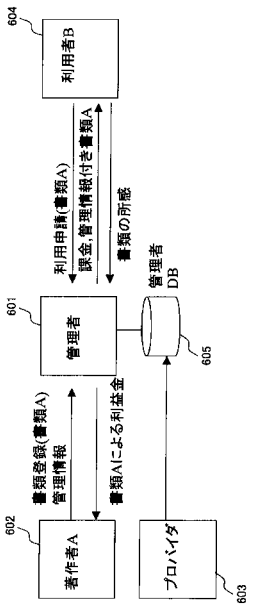
【図４９】



【図５０】



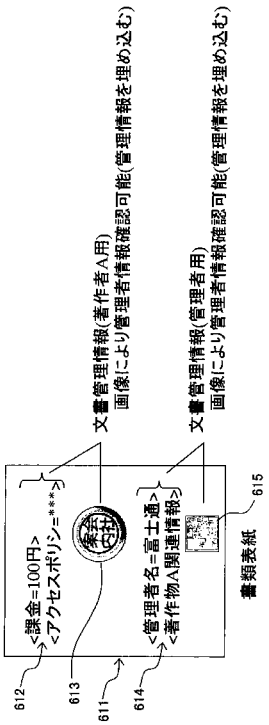
【図５１】



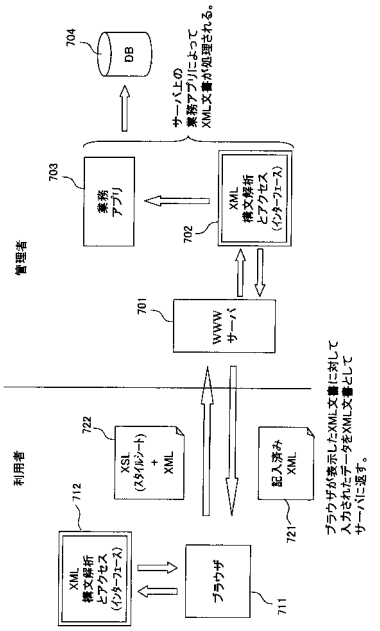
【図５２】

著作者Aが提出した管理情報		管理者が生成した管理情報	
文書名	制御情報	課金	利用者ログ(利用者名,日時,回数)	人気度
Doc1	アクセスポリシー	100円	A,2001.8.20,1	1
Doc2	アクセスポリシー	20円	B,2001.8.21,2	2

【図５３】



【図５４】



【図５５】

XMLコード例 (demo.xml)

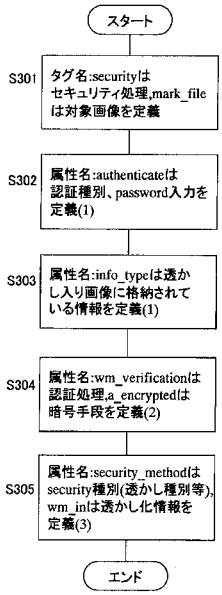
```
<?xml version="1.0"?>
<?xml-stylesheet type="text/xsl"href="demo.xsl"?>
<xmldocument>
    <open1>The secret will show as below </open1>
        <security authenticate="password"info_type="secret,authentication"> ****** </security>  (1)
        <security wm_verification="2001.8.30"a_encrypted="DES"></security>  (2)
            <mark_filewm_in="t0"security_method="invisible_watermark_f">mark.gif </mark_file>  (3)
</xmldocument>
```

【図５６】

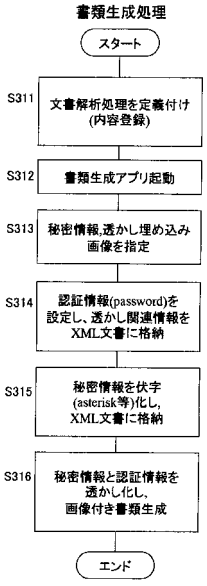
スタイルシート例 (demo.xsl)

```
<?xml version="1.0"?>
<xsl:stylesheet xmlns:xsl="http://www.w3.org/TR/WD-xsl">
<xsl:template match="/">
<html>
    <body>
        <xsl:apply-templates select="xmldocument"/>
    </body>
</html>
</xsl:template>
<xsl:template match="xmldocument">
    <xsl:value-of select="open1"/>
    <xsl:value-of select="security"/>
    <img>
        <xsl:attribute name="src">
            <xsl:value-of select="mark_file"/>
        </xsl:attribute>
    </img>
</xsl:template>
</xsl:stylesheet>
```

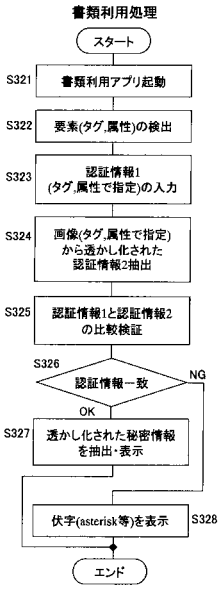
【図５７】



【図５８】



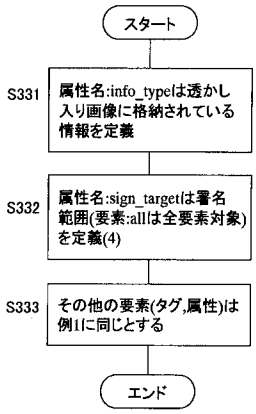
【図５９】



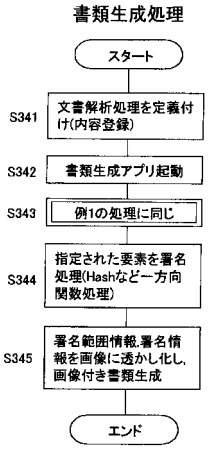
【図６０】

```
<?xml version="1.0"?>
<?xml-stylesheet type="text/xsl"href="demo.xsl"?>
<xmldocument>
    <open1>The secret will show as below </open1>
        <security authenticate="password"info_type="secret,authentication,sign"> ****** </security>
        <security wm_verification="2001.8.30"a_encrypted="DES"></security>
        <mark_file  wm_in="f0"security_method="invisible_watermark_F">mark.gif </mark_file>
        <security sign_target="all"></security>  (4)
</xmldocument>
```

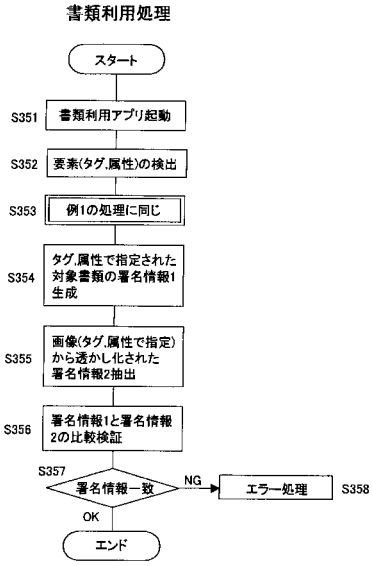
【図６１】



【図６２】



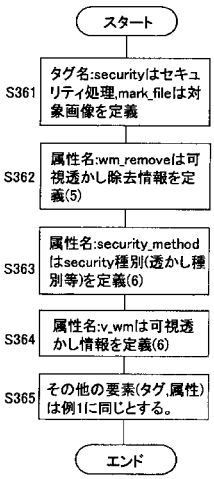
【図６３】



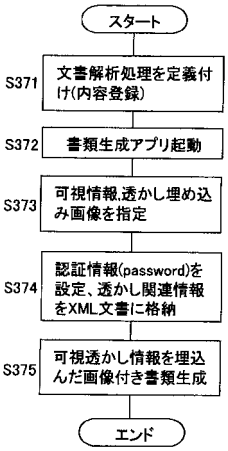
【図６４】

```
<?xml version="1.0"?>
<?xml-stylesheet type="text/xsl"href="demo.xsl"?>
<xmldocument>
<open1>The visible will show as below </open1>
<security authenticate="password"wm_remove="@password">(5)</security>
<security wm_verification="2001.8.30"a_encrypted="DES"></security>
<mark_file v_wm="FI"security_method="visible_watermark_f">mark.gif </mark_file> (6)
</xmldocument>
```

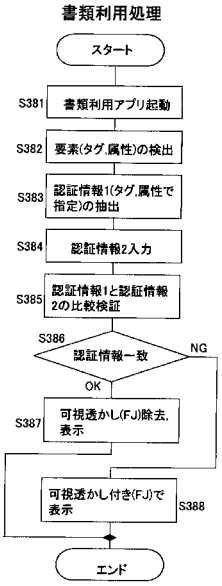
【図６５】



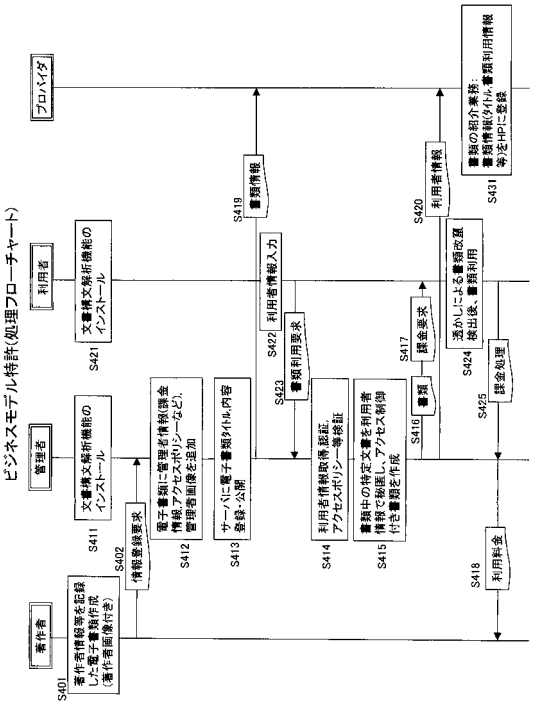
【図６６】



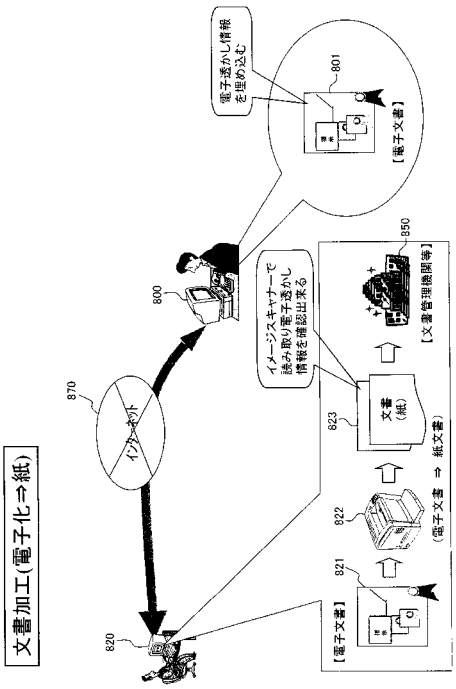
【図６７】



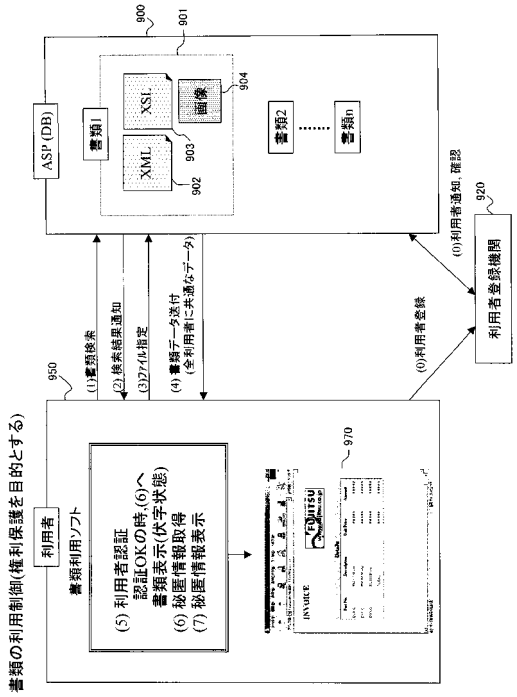
【図６８】



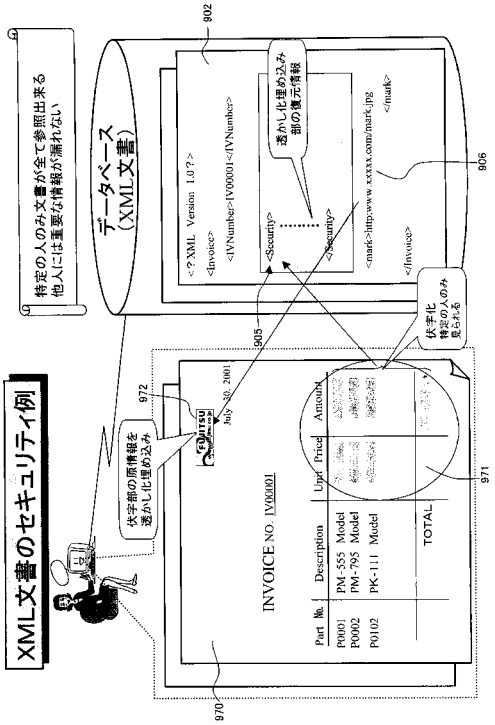
【図６９】



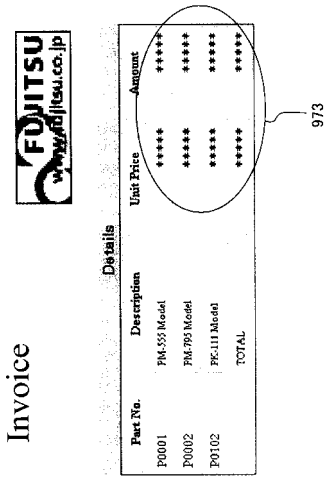
【図７０】



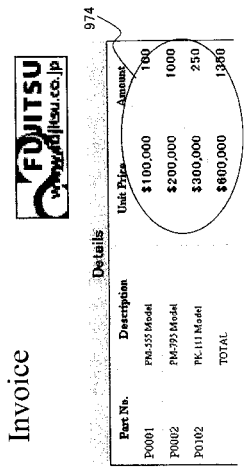
【図７１】



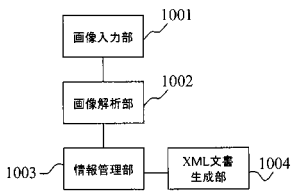
【図７２】



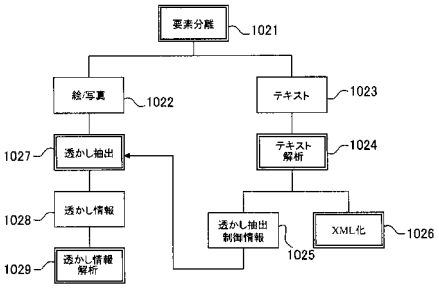
【図７３】



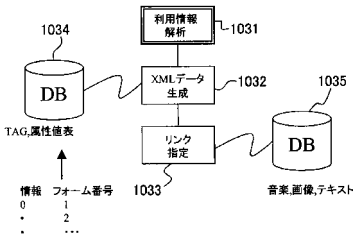
【図７４】



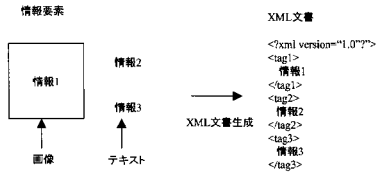
【図７５】



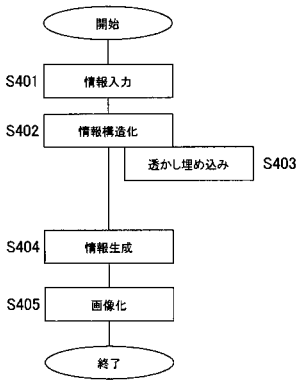
【図７６】



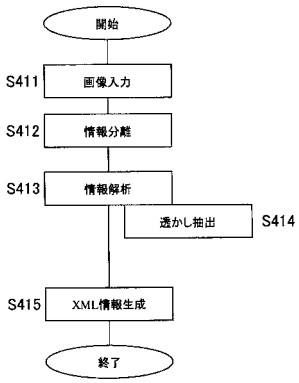
【図７７】


情報要素
情報1
情報2
情報3
画像
テキスト
XML文書生成
XML文書
<?xml version="1.0"?>
<tag1>
情報1
</tag1>
<tag2>
情報2
</tag2>
<tag3>
情報3
</tag3>

【図７８】


開始
S401
情報入力
S402
情報構造化
透かし埋め込み
S403
S404
情報生成
S405
画像化
終了

【図７９】


開始
S411
画像入力
S412
情報分離
S413
情報解析
透かし抽出
S414
S415
XML情報生成
終了

フロントページの続き

合議体
審判長　小曳　満昭
審判官　加内　慎也
審判官　田口　英雄

(56)参考文献　特開２００１－１３４１８０（ＪＰ，Ａ）
特開２００１－１４７９３４（ＪＰ，Ａ）
特開２００１－１７７７１７（ＪＰ，Ａ）
特開２００１－２１８００８（ＪＰ，Ａ）
特開平１０－３２２４９２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F17/21-17/26