(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4993674号
(P4993674)
(45)発行日　平成24年8月8日(2012.8.8)　(24)登録日　平成24年5月18日(2012.5.18)

(51)Int.Cl.　　F I
H04L 9/32 (2006.01)　　H04L 9/00 675B
G09C 1/00 (2006.01)　　G09C 1/00 660D

請求項の数 16　(全 21 頁)

(21)出願番号　特願2006-232812(P2006-232812)
(22)出願日　平成18年8月29日(2006.8.29)
(65)公開番号　特開2007-104643(P2007-104643A)
(43)公開日　平成19年4月19日(2007.4.19)
審査請求日　平成21年8月31日(2009.8.31)
(31)優先権主張番号　特願2005-263074(P2005-263074)
(32)優先日　平成17年9月9日(2005.9.9)
(33)優先権主張国　日本国(JP)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(72)発明者　須賀　祐治
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

最終頁に続く

(54)【発明の名称】情報処理装置、検証処理装置及びそれらの制御方法、コンピュータプログラム及び記憶媒体

(57)【特許請求の範囲】
【請求項１】
電子文書を領域分割して被署名データを生成する第１の生成手段と、
前記被署名データの第１のダイジェスト値及び該被署名データを識別するための識別情報を生成する第２の生成手段と、
前記電子文書から得られた、複数の前記第１のダイジェスト値及び識別情報に基づき、署名情報を生成する第３の生成手段と、
前記署名情報と前記被署名データとにより第１の署名された電子文書を生成する第４の生成手段と
を備え、
前記第３の生成手段は、前記電子文書より得られた、複数の前記第１のダイジェスト値及び識別情報と、暗号化鍵とを用いて署名値を生成し、該署名値と該複数の第１のダイジェスト値及び前記識別情報とにより前記署名情報を生成することを特徴とする情報処理装置。
【請求項２】
前記被署名データの選択を受け付ける選択受付手段を備え、
前記第３の生成手段は、前記選択受付手段により選択を受け付けた被署名データの前記第１のダイジェスト値及び前記識別情報に基づき前記署名情報を生成することを特徴とする請求項１に記載の情報処理装置。
【請求項３】

前記電子文書のうち、所定領域の指定を受け付ける領域指定受付手段を更に備え、
前記第１の生成手段は、前記領域指定受付手段により指定された前記所定領域について前記被署名データを生成することを特徴とする請求項１又は２に記載の情報処理装置。
【請求項４】
請求項１乃至３のいずれか１項に記載の情報処理装置により生成された第１の署名された電子文書に基づき、電子文書の検証を行う検証処理装置であって、
前記第１の署名された電子文書から、前記署名情報を抽出する抽出手段と、
前記署名情報における前記第１のダイジェスト値及び識別情報の改竄性の有無を判定する判定手段と、
前記判定手段により、前記第１のダイジェスト値及び前記識別情報が改竄されていないと判定された場合に、前記識別情報に基づき、前記第１の署名された電子文書より前記被署名データを取得する取得手段と、
前記被署名データの第２のダイジェスト値を算出する算出手段と、
前記第１のダイジェスト値と前記第２のダイジェスト値とを比較する比較手段と、
前記比較の結果に基づいて検証結果を生成する検証結果生成手段と
を備えることを特徴とする検証処理装置。
【請求項５】
前記判定手段は、前記署名情報に含まれる前記署名値を復号鍵を用いて復号して得られた結果が、前記第１のダイジェスト値及び前記識別情報と一致するか否かに基づいて、前記第１のダイジェスト値及び前記識別情報が改竄されたか否かを判定することを特徴とする請求項４に記載の検証処理装置。
【請求項６】
前記取得手段は、複数の前記識別情報のうち、いずれかの識別情報に対応する被署名データが取得できない場合であっても、他の識別情報に対応する被署名データが取得できる場合には、該被署名データを取得することを特徴とする請求項４又は５に記載の検証処理装置。
【請求項７】
前記第１の署名された電子文書に操作を施す操作手段と、
前記操作が施された前記第１の署名された電子文書について、第２の署名された電子文書を生成する第５の生成手段とを更に備え、
前記操作手段において、前記第１の署名された電子文書に含まれる被署名データのいずれかが選択されて電子文書が再構成された場合に、前記第５の生成手段は、前記再構成された電子文書について、前記署名情報と前記操作において選択された被署名データとにより前記第２の署名された電子文書を生成することを特徴とする請求項４乃至６のいずれか１項に記載の検証処理装置。
【請求項８】
第１の生成手段が、電子文書を領域分割して被署名データを生成する第１の生成工程と、
第２の生成手段が、前記被署名データの第１のダイジェスト値及び該被署名データを識別するための識別情報を生成する第２の生成工程と、
第３の生成手段が、前記電子文書から得られた、複数の前記第１のダイジェスト値及び識別情報に基づき、署名情報を生成する第３の生成工程と、
第４の生成手段が、前記署名情報と前記被署名データとにより署名された電子文書を生成する第４の生成工程と
を備え、
前記第３の生成工程では、前記電子文書より得られた、複数の前記第１のダイジェスト値及び識別情報と、暗号化鍵とを用いて署名値を生成し、該署名値と該複数の第１のダイジェスト値及び前記識別情報とにより前記署名情報を生成することを特徴とする情報処理装置の制御方法。
【請求項９】

選択受付手段が、前記被署名データの選択を受け付ける選択受付工程を更に備え、
前記第３の生成工程では、前記選択受付工程において選択を受け付けた被署名データの前記第１のダイジェスト値及び前記識別情報に基づき前記署名情報を生成することを特徴とする請求項８に記載の情報処理装置の制御方法。
【請求項１０】
領域指定受付手段が、前記電子文書のうち、所定領域の指定を受け付ける領域指定受付工程を更に備え、
前記第１の生成工程では、前記領域指定受付工程において指定された前記所定領域について前記被署名データを生成することを特徴とする請求項８又は９に記載の情報処理装置の制御方法。
【請求項１１】
請求項８乃至１０のいずれか１項に記載の方法により生成された署名された電子文書に基づき、電子文書の検証を行う検証処理装置の制御方法であって、
抽出手段が、前記署名された電子文書から、前記署名情報を抽出する抽出工程と、
判定手段が、前記署名情報における前記第１のダイジェスト値及び識別情報の改竄性の有無を判定する判定工程と、
取得手段が、前記判定工程において、前記第１のダイジェスト値及び前記識別情報が改竄されていないと判定された場合に、前記識別情報に基づき、前記署名された電子文書より前記被署名データを取得する取得工程と、
算出手段が、前記被署名データの第２のダイジェスト値を算出する算出工程と、
比較手段が、前記第１のダイジェスト値と前記第２のダイジェスト値とを比較する比較工程と、
検証結果生成手段が、前記比較の結果に基づいて検証結果を生成する検証結果生成工程と
を備えることを特徴とする検証処理装置の制御方法。
【請求項１２】
前記判定工程では、前記署名情報に含まれる前記署名値を復号鍵を用いて復号して得られた結果が、前記第１のダイジェスト値及び前記識別情報と一致するか否かに基づいて、前記第１のダイジェスト値及び前記識別情報が改竄されたか否かを判定することを特徴とする請求項１１に記載の検証処理装置の制御方法。
【請求項１３】
前記取得工程では、複数の前記識別情報のうち、いずれかの識別情報に対応する被署名データが取得できない場合であっても、他の識別情報に対応する被署名データが取得できる場合には、該被署名データを取得することを特徴とする請求項１１又は１２に記載の検証処理装置の制御方法。
【請求項１４】
操作手段が、前記第１の署名された電子文書に操作を施す操作工程と、
第５の生成手段が、前記操作が施された前記第１の署名された電子文書について、第２の署名された電子文書を生成する第５の生成工程とを更に備え、
前記操作工程において、前記第１の署名された電子文書に含まれる被署名データのいずれかが選択されて電子文書が再構成された場合に、前記第５の生成工程では、前記再構成された電子文書について、前記署名情報と前記操作において選択された被署名データとにより前記第２の署名された電子文書を生成することを特徴とする請求項１１乃至１３のいずれか１項に記載の検証処理装置の制御方法。
【請求項１５】
請求項８乃至１４のいずれか１項に記載の方法をコンピュータに実行させるためのコンピュータプログラム。
【請求項１６】
請求項１５に記載のコンピュータプログラムを記憶したコンピュータで読み取り可能な記憶媒体。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置、検証処理装置及びそれらの制御方法、コンピュータプログラム及び記憶媒体に関する。
【背景技術】
【０００２】
近年、コンピュータとそのネットワークの急速な発達及び普及により、文字データ、画像データ、音声データなど、多種の情報がデジタル化されている。デジタルデータは、経年変化などによる劣化がなく、いつまでも完全な状態で保存できる一方、容易に複製や編集・加工を施すことが可能である。
【０００３】
こうしたデジタルデータの複製、編集、加工はユーザにとって大変有益である反面、デジタルデータの保護が大きな問題となっている。特に、文書や画像データがインターネットなどの広域ネットワーク網を通して流通する場合、デジタルデータは改変が容易であるため、第三者によってデータが改竄される危険性がある。
【０００４】
そこで、送信されてきたデータが改竄されたかどうかを受信者が検出するために、改竄防止用の付加データを検証する方式としてデジタル署名という技術が提案されている。デジタル署名技術は、データ改竄だけではなく、インターネット上でのなりすまし、否認などを防止する効果も持ち合わせている。
【０００５】
以降では、デジタル署名、ハッシュ関数、公開鍵暗号、及び公開鍵認証基盤について詳細に説明する。
【０００６】
[デジタル署名]
図１４は、署名作成処理および署名検証処理を説明するための模式図であり、同図を参照して説明を行う。デジタル署名データ生成にはハッシュ関数と公開鍵暗号とが用いられる。
ここで、秘密鍵をＫｓ（２１０６）、公開鍵をＫｐ（２１１１）とすれば、送信者はデータＭ（２１０１）にハッシュ処理２１０２を施して固定長データであるダイジェスト値Ｈ（Ｍ）（２１０３）を算出することができる。次に、秘密鍵Ｋｓ（２１０６）を用いて固定長データＨ（Ｍ）に署名処理２１０４を施せば、デジタル署名データＳ（２１０５）を作成することができる。そして、受信者には、このデジタル署名データＳ（２１０５）とデータＭ（２１０１）とが送信される。
【０００７】
一方、受信者は、受信したデジタル署名データＳ（２１１０）を公開鍵Ｋｐ（２１１１）を用いて変換（復号）する。また、受信したデータＭ（２１０７）にハッシュ処理２１０８を施して、固定長のダイジェスト値：Ｈ（Ｍ）２１０９を生成する。検証処理２１１２では、復号により得られたデータと、ダイジェスト値Ｈ（Ｍ）とが一致するか否かを検証する。そして、この検証により両データが一致しないならば、改竄が行われたことを検出できる。
【０００８】
デジタル署名にはＲＳＡ、ＤＳＡ（詳細は後述）などの公開鍵暗号方式が用いられている。これらのデジタル署名の安全性は、秘密鍵の所有者以外のエンティティが、署名を偽造、もしくは秘密鍵を解読することが計算的に困難であることに基づいている。
【０００９】
[ハッシュ関数]
次に、ハッシュ関数について説明する。ハッシュ関数は署名対象データを非可逆に圧縮して署名付与処理時間を短縮するためにデジタル署名処理とともに利用される。つまり、

ハッシュ関数は任意の長さのデータMに処理を行い、一定の長さの出力データH（M）を生成する機能を持っている。ここで、出力H（M）を平文データMのハッシュデータと呼ぶ。

【００１０】

特に、一方向性ハッシュ関数は、データMを与えた時、H（M'）＝H（M）となる平文データM'の算出が計算量的に困難であるという性質を持っている。上記一方向性ハッシュ関数としてはＭＤ２、ＭＤ５、ＳＨＡ－１などの標準的なアルゴリズムが存在する。

【００１１】

[公開鍵暗号]

次に、公開鍵暗号について説明する。公開鍵暗号は２つの異なる鍵を利用し、片方の鍵で暗号処理したデータは、もう片方の鍵でしか復号処理できないという性質を持っている。上記２つの鍵のうち、一方の鍵は公開鍵と呼ばれ、広く公開するようにしている。また、もう片方の鍵は秘密鍵と呼ばれ、本人のみが持つ鍵である。

【００１２】

公開鍵暗号方式を用いたデジタル署名としては、ＲＳＡ署名、ＤＳＡ署名、Schnorr署名などが挙げられる。ここでは例として、非特許文献１に記載されているＲＳＡ署名を説明する。また、非特許文献２に記載されているＤＳＡ署名についても併せて説明する。

【００１３】

[ＲＳＡ署名]

素数ｐ、ｑを生成しｎ＝ｐｑとおく。λ（ｎ）をｐ－１とｑ－１の最小公倍数とする。λ（ｎ）と素な適当なｅを選び、ｄ＝１／ｅ　（ｍｏｄ　λ（ｎ））とおく。公開鍵をｅおよびｎとし、秘密鍵をｄとする。またH（）をハッシュ関数とする。

【００１４】

[ＲＳＡ署名作成]文書Mに対する署名の作成手順

ｓ：＝H（M）＾ｄ（ｍｏｄ　ｎ）を署名データとする。

【００１５】

[ＲＳＡ署名検証] 文書Mに対する署名 (s,T) の検証手順

H（M）＝ｓ＾ｅ（ｍｏｄ　ｎ）かどうか検証する。

【００１６】

[ＤＳＡ署名]

p，q を素数とし、 p-１は qを割り切るとする。ｇをZ_p*（位数pの巡回群Z_p から０を省いた乗法群）から任意に選択した、位数qの元（生成元）とする。 Z_p*から任意に選択したxを秘密鍵とし、それに対する公開鍵yをy:= g＾x mod pとおく。 H()をハッシュ関数とする。

【００１７】

[ＤＳＡ署名作成]文書Mに対する署名の作成手順

１）αをZ_q から任意に選択し、T:= (g＾α mod p) mod qとおく。

２）c:= H(M) とおく。

３）s:=α＾-１(c + xT) mod q とおき、(s,T) を署名データとする。

【００１８】

[ＤＳＡ署名検証] 文書Mに対する署名 (s,T) の検証手順

T = (g＾(h(M) s^-１) y＾(T s^-１)mod p) mod q かどうか検証する。

【００１９】

[公開鍵認証基盤]

クライアント・サーバ間の通信においてサーバのリソースにアクセスする際には、利用者認証が必要であるが、その一つの手段として ITU-U 勧告の X.５０９ 等の公開鍵証明書がよく用いられている。公開鍵証明書は公開鍵とその利用者との結びつけを保証するデータであり、認証機関と呼ばれる信用のおける第３者機関によるデジタル署名が施されたものである。例えば、ブラウザで実装されている SSL (Secure Sockets Layer) を用いた利用者認証方式は、ユーザの提示してきた公開鍵証明書内に含まれる公開鍵に対応する秘

密鍵をユーザが持っているかどうか確認することで行われる。

【００２０】

公開鍵証明書は認証機関による署名が施されていることで、公開鍵証明書内に含まれているユーザやサーバの公開鍵を信頼することができる。そのため、認証機関が署名作成のために用いる秘密鍵が漏洩され、或いは脆弱になった場合、この認証機関から発行されたすべての公開鍵証明書は無効になってしまう。認証機関によっては膨大な数の公開鍵証明書を管理しているため、管理コストを下げるためにさまざまな提案が行われている。後述する本発明によれば、発行する証明書数を抑え、かつ公開鍵リポジトリとしてのサーバアクセスを軽減する効果がある。

【００２１】

公開鍵証明書の一例である非特許文献３に記載のITU-U 勧告X.５０９ v.３では被署名データとして証明対象となるエンティティ（Subject）のIDおよび公開鍵情報が含まれている。そして、これらの被署名データにハッシュ関数を施したダイジェストについて、前述したRSAアルゴリズムなどの署名演算により署名データが生成される。また、被署名データにはextensions というオプショナルなフィールドが設けられ、アプリケーション又はプロトコル独自の新しい拡張データを含ませることが可能である。

【００２２】

図１５は、X.５０９ v.３で規定されるフォーマットを示しているおり、以下、それぞれのフィールドに表示される情報を説明する。version１５０１は X.５０９ のバージョンが入る。このフィールドはオプショナルであり、省略された場合は ｖ１ を表わす。serialNumber１５０２は認証機関がユニークに割り当てるシリアル番号が入る。signature１５０３は、公開鍵証明書の署名方式が入る。issuer１５０４は、公開鍵証明書の発行者である認証機関の X.５００ 識別名が入る。validity１５０５は、公開鍵の有効期限（開始日時と終了日時）が入る。

【００２３】

subject１５０６は、本証明書内に含まれる公開鍵に対応する秘密鍵の所有者の X.５００ 識別名が入る。subjectPublicKeyInfo１５０７は、証明する公開鍵が入る。issuerUniqueIdentifier１５０８及びsubjectUniqueIdentifier１５０９は、ｖ２ から追加されたオプショナルなフィールドであり、それぞれ認証機関の固有識別子、所有者の固有識別子が入る。

【００２４】

extensions１５１０は、ｖ３ で追加されたオプショナルなフィールドであり、拡張型（extnId)１５１１、クリティカルビット (critical)１５１２及び拡張値 (extnValue)１５１３の３つの値の集合が入る。ｖ３ 拡張フィールドには、X.５０９ で定められた標準の拡張型だけでなく、独自の新しい拡張型も組み込むことが可能である。そのため ｖ３ 拡張型をどう認識するかはアプリケーション側に依存することとなる。クリティカルビット１５１２はその拡張型が必須であるかまたは無視可能かを表わすものである。

【００２５】

以上、デジタル署名、ハッシュ関数、公開鍵暗号、及び公開鍵認証基盤について説明した。

【００２６】

前述のデジタル署名技術を用いて、署名対象となるテキストデータを複数のテキストデータに分割し、署名文単位に電子署名を付加する方式が提案されている（特許文献１を参照）。この提案方式によれば、電子署名されたテキストデータから一部を引用しても、該引用した一部の文についての検証処理が可能となる。

【特許文献１】特開平１０-００３２５７号公報

【非特許文献１】R.L. Rivest, A. Shamir and L. Adleman: "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, v. ２１, n. ２, pp. １２０-１２６, Feb １９７８.

【非特許文献２】Federal Information Processing Standards (FIPS) １８６-２, Digit

al Signature Standard (DSS) , January ２０００
【非特許文献３】ITU-T Recommendation X.５０９/ISO/IEC ９５９４-８: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".
【発明の開示】
【発明が解決しようとする課題】
【００２７】
上記の提案方式では、テキストデータのみを署名対象データとして扱っているが、近年のデジタルデータの多様化により、複数の種類のコンテンツで構成された複合コンテンツに対してデジタル署名を施すことも考えられる。係る複合コンテンツを一つのバイナリデータの塊として処理し、圧縮処理などを経てデジタル署名を施す場合、第三者がコンテンツをサブコンテンツに分解して再配布する際に、該サブコンテンツにおける署名データは検証可能状態にならない。
【００２８】
これを回避するために、上記提案方式と同様にテキストデータに限らず署名対象サブコンテンツごとにデジタル署名を施すことも考えられるが、その場合には、署名生成・署名検証ともに暗号処理には多大の計算コストがかかる。よって、サブコンテンツ数が多くなるにつれ処理が増大してしまうという別の問題が発生する。
【００２９】
そこで本発明は、テキストデータのみならず多様なフォーマットで格納されたデジタルデータの複合体に対し、その一部分であるサブコンテンツが分離されて存在しても署名検証が可能とすることを目的とする。かつ、署名生成および署名検証処理の計算量がサブコンテンツの分割数に比例せず、一定となるような署名技術を提供することを目的とする。
【課題を解決するための手段】
【００３０】
上記課題をまとめて、又は、個々に解決する本発明は、情報処理装置であって、
電子文書を領域分割して被署名データを生成する第１の生成手段と、
前記被署名データの第１のダイジェスト値及び該被署名データを識別するための識別情報を生成する第２の生成手段と、
前記電子文書から得られた、複数の前記第１のダイジェスト値及び識別情報に基づき、署名情報を生成する第３の生成手段と、
前記署名情報と前記被署名データとにより第１の署名された電子文書を生成する第４の生成手段とを備え、
前記第３の生成手段は、前記電子文書より得られた、複数の前記第１のダイジェスト値及び識別情報と、暗号化鍵とを用いて署名値を生成し、該署名値と該複数の第１のダイジェスト値及び前記識別情報とにより前記署名情報を生成することを特徴とする。
【００３１】
また、上記第１の署名された電子文書に基づき、電子文書の検証を行う検証処理装置であって、
前記第１の署名された電子文書から、前記署名情報を抽出する抽出手段と、
前記署名情報における前記第１のダイジェスト値及び識別情報の改竄性の有無を判定する判定手段と、
前記判定手段により、前記第１のダイジェスト値及び前記識別情報が改竄されていないと判定された場合に、前記識別情報に基づき、前記第１の署名された電子文書より前記被署名データを取得する取得手段と、
前記被署名データの第２のダイジェスト値を算出する算出手段と、
前記第１のダイジェスト値と前記第２のダイジェスト値とを比較する比較手段と、
前記比較結果に基づいて検証結果を生成する検証結果生成手段と
を備えることを特徴とする。
【発明の効果】

【００３２】
以上説明したように、本発明によれば、テキストデータだけではなく多様なフォーマットで格納されたデジタルデータの複合体に対して、その一部分であるサブコンテンツが分離されて存在しても署名検証が可能となる。かつ、効率的に署名生成および署名検証処理が可能となる。
【発明を実施するための最良の形態】
【００３３】
以下、図面を参照して、本発明の好適な実施形態を説明する。
【００３４】
＜第１の実施形態＞
本実施形態に対応する署名作成処理及び署名検証処理は、電子文書生成工程と電子文書操作工程とで構成される。具体的に、電子文書生成工程では、紙文書をスキャンして生成された画像データをサブコンテンツに分割し、ユーザが所望のサブコンテンツ群にデジタル署名を施した複合コンテンツ（以下、電子文書と呼ぶ）を生成する。次に、電子文書操作工程では、電子文書をサブコンテンツに展開し、検証が必要なサブコンテンツに対する署名情報の検証を行い、閲覧、印刷などのコンテンツ消費処理やコンテンツ再構成処理などを行う。
【００３５】
図１は、本実施形態に対応するシステムの構成の一例を示す図である。図１に示されるシステムは、スキャナ１０１、電子文書を生成・検証する処理装置としてのコンピュータ装置１０２、電子文書を編集加工するコンピュータ装置１０３及び電子文書を印刷する印刷装置１０４がネットワーク１０５に接続されて構成されている。
【００３６】
図２は、本実施形態に対応するシステムの機能構成の一例を示す機能ブロック図である。図２において、画像入力装置２０１には画像データが入力される。鍵情報２０２は、電子署名作成用の暗号化鍵および電子署名検証用の復号鍵である。情報処理装置としての電子文書生成装置２０３は、入力画像データと鍵情報２０２の暗号化鍵から、入力画像データに署名を付加して、電子文書２０４を生成する。作成された電子文書２０４には、検証処理装置としての電子文書操作装置２０５上で、鍵情報２０２の復号鍵を用いた電子文書の検証に加え、データ加工、編集、印刷等の操作が行われる。以下、電子署名の方法は公開鍵暗号方式に準じて説明する．このとき、鍵情報２０２の暗号化鍵は秘密鍵４０６、鍵情報２０２の復号鍵は公開鍵４１４に対応する。
【００３７】
図３は、電子文書生成装置２０３および電子文書操作装置２０５の内部ハードウエア構成の一例である。３０１はソフトウエアを実行することで装置の大部分を制御するＣＰＵである。３０２は、ＣＰＵ３０１が実行するソフトウエアやデータを一時記憶するメモリである。３０３は、ソフトウエアやデータを保存するハードディスクである。３０４は、キーボードやマウス、スキャナなどの入力情報を受け取り、またディスプレイやプリンタに情報を出力する入出力（Ｉ／Ｏ）部である。
【００３８】
[電子文書生成工程]
次に、本実施形態に対応する処理について説明する。図４は、本実施形態に対応する処理の一例を示す機能ブロック図である。図４で示されるように、本実施形態に対応する処理は、大きく電子文書生成工程４０１と、電子文書操作工程４０２とで構成される。
【００３９】
本実施形態に対応する電子文書生成工程４０１では、紙文書入力工程４０４において紙文書４０３が入力される。次に、中間電子文書生成工程４０５において、紙文書４０３を解析し中間電子文書が生成される。署名情報生成工程４０７において、中間電子文書および秘密鍵４０６から署名情報が生成される。署名情報付加工程４０８において、中間電子文書と署名情報とが関連付けられる。電子文書アーカイブ工程４０９において、中間電子

文書と署名情報とが統合され電子文書４１１が生成される。この電子文書４１１は、図２の電子文書２０４に対応する。電子文書送信工程４１０において、電子文書４１１が電子文書操作工程４０２に送信される。

【００４０】

次に、電子文書操作工程４０２では、電子文書受信工程４１２において電子文書４１１が受信される。電子文書展開工程４１３において、受信した電子文書４１１が展開され、中間電子文書と署名情報が取得される。署名情報検証工程４１５において、中間電子文書、署名情報、公開鍵４１４をもとに検証が行われる。文書操作工程４１６では、展開された電子文書に加工、編集、印刷などの操作が行われる。

【００４１】

以下、図４の各機能ブロックの詳細を更に説明する。まず、図５及び図６を参照して、中間電子文書生成工程４０５の詳細を説明する。図５は本実施形態に対応する中間電子文書生成工程４０５における処理の一例を示すフローチャートである。図６は、電子データ及び領域分割処理結果の一例を示す図である。

【００４２】

図５において、ステップＳ５０１では、紙文書入力工程４０４から得られたデータを電子化し、電子データを生成する。図６（ａ）は生成された電子データの一例を示す。

【００４３】

次に、ステップＳ５０２では電子データを属性ごとに領域分割する。ここでいう属性とは、文字、写真、表、線画があげられる。

【００４４】

領域分割処理は、例えば電子データ中の黒画素の８連結輪郭塊や白画素の４連結輪郭塊といった集合を抽出し、その形状、大きさ、集合状態などから、文字、絵や図、表、枠、線といった特徴名で領域を抽出することができる。このような手法は、例えば米国特許第５６８０４７８号公報に記載されている。なお、領域分割処理の実現方法は、これに限られるものではなく、他の方法を適用しても良い。

【００４５】

図６（ｂ）は、抽出した特徴量をもとに属性を判別し、領域分割を行った結果の一例を示す。ここで、各領域の属性は、６０２、６０４、６０５及び６０６が文字領域、６０３がカラー写真領域となっている。

【００４６】

次にステップＳ５０３では、ステップＳ５０２において得られた領域を、領域ごとに文書情報を生成する。文書情報とは属性、ページの位置座標等のレイアウト情報、分割された領域の属性が文字であれば文字コード列や、段落や表題などの文書論理構造等があげられる。

【００４７】

次にステップＳ５０４では、ステップＳ５０２において得られた領域を、領域ごとに伝達情報に変換する。伝達情報とは、レンダリングに必要な情報のことである。具体的には解像度可変のラスタ画像、ベクタ画像、モノクロ画像、カラー画像、各伝達情報のファイルサイズ、分割領域の属性が文字であれば文字認識した結果のテキスト、個々の文字の位置、フォント、文字認識によって得られた文字の信頼度等である。図６（ｂ）を例とすれば、文字領域６０２、６０４、６０５及び６０６はベクタ画像に、カラー写真領域６０３はカラーラスタ画像に変換されるものとする。

【００４８】

次にステップＳ５０５では、ステップＳ５０２で分割された領域と、ステップＳ５０３で生成された文書情報と、ステップＳ５０４で得られた伝達情報とを関連付ける。関連付けた情報はツリー構造で記述される。以降、以上において生成された伝達情報及び文書情報を構成要素と呼ぶ。

【００４９】

ステップＳ５０６では、以上において生成された構成要素を中間電子文書として保存す

る。保存の形式はツリー構造を表現可能な形式であればよい。本実施形態は構造化文書の一例であるＸＭＬで保存する。

【００５０】

次に、図４の署名情報生成工程４０７について説明する。本工程では、先に生成された中間電子文書の構成要素に対し、デジタル署名を生成する。図８は本実施形態における署名情報生成工程のフローチャートであり、以下、署名情報生成工程４０７について、図８を参照して説明する。

【００５１】

まず、ステップＳ８０１では、被署名データのダイジェスト値を、被署名データ毎に夫々生成する。ここで、被署名データとは、中間電子文書中に含まれる署名対象データのことであり、後述する図７（ａ）における伝達情報ａ（７０１）、伝達情報ｂ（７０２）、或いは文書情報（７０３）であると考えることができる。また、ダイジェスト値を生成するために、本実施形態ではハッシュ関数を適用する。ハッシュ関数については、［背景技術］の項において既に説明したので、ここでの詳細な説明は省略する。

【００５２】

次に、ステップＳ８０２では、被署名データの識別情報を、被署名データ毎に生成する。ここで、識別情報としては、被署名データをユニークに識別可能なものであれば良い。例えば、本実施形態では、被署名データの識別情報として、ＲＦＣ２３９６で規定されているＵＲＩを適用するものとするが、本発明はこれに限定されることなく、種々の値を識別情報として適用可能であることは明らかである。

【００５３】

そして、ステップＳ８０３では、全ての署名対象データに対してステップＳ８０１及びステップＳ８０２が適用されたか否かが判定される。全ての署名対象データに対してステップＳ８０１及びステップＳ８０２が適用された場合には（ステップＳ８０３において「ＹＥＳ」）、処理をステップＳ８０４に進め、さもなければステップＳ８０１に戻る。

【００５４】

ステップＳ８０４では、ステップＳ８０１で生成された同一の電子文書についての全てのダイジェスト値、及び、ステップＳ８０２で生成された全ての識別情報に対し、秘密鍵４０６を用いて署名処理を実行し、署名値を算出する。署名値を算出するために、本実施形態では［背景技術］の項において説明したデジタル署名を適用する。デジタル署名の具体的な演算処理については詳細な説明は省略する。図１４（ａ）で示した署名作成処理フローにおけるデータＭ（２１０１）が、ここではステップＳ８０１で生成された全てのダイジェスト値、及び、ステップＳ８０２で生成された全ての識別情報（このデータ群を集約データと呼ぶ）に該当する。同じく秘密鍵Ｋｓ２１０６は図４の秘密鍵４０６に対応する。

【００５５】

続いてステップＳ８０５では、集約データ（ステップＳ８０１で生成された全てのダイジェスト値とステップＳ８０２で生成された全ての識別情報）及びステップＳ８０４で生成された署名値を用いて署名情報を構成し、署名生成処理を終了する。

なお、ステップＳ８０４における署名値の算出処理は、生成された全てのダイジェスト値や全ての識別情報について行わず、生成されたダイジェスト値及び識別情報の一部（すなわち、生成された複数のダイジェスト値及び識別情報）について行っても良い。

【００５６】

この場合、例えば、オリジナルコンテンツにおいて再利用される可能性の高いサブコンテンツを自動或いはユーザによる手動で選択し、該サブコンテンツに関するダイジェスト値や識別情報について署名値を算出してもよい。その場合、ステップＳ８０５では、署名値の算出に利用された該一部のダイジェスト値及び識別情報と、算出した署名値とを用いて署名情報が構成される。なお、複数のダイジェスト値及び識別情報を用いて署名値を算出する場合であっても、コンテンツ全体に対し、署名値の演算処理を１回で済ませることができる。

【００５７】
ここで、本実施形態に対応する電子文書４１１の構成について図９を参照して説明する。図９は、本実施形態に対応する電子文書４１１の構成の一例を示す図である。図９（ａ）は、電子文書４１１全体の構成を示す。ここで、９０１は署名情報、９０２は被署名データ１、９０３は被署名データ２をそれぞれ示す。図９（ｂ）は、図９（ａ）中の署名情報９０１の詳細な構成の一例を示す。ここで、９０４は署名値、９０５は被署名データ１の識別情報、９０６は被署名データ１のダイジェスト値、９０７は被署名データ２の識別情報、９０８は被署名データ２のダイジェスト値をそれぞれ示す。９０５から９０８で構成されるデータは集約データ９０９に該当する。

【００５８】
図９（ａ）に示す例では、２つの被署名データ１（９０２）及び被署名データ２（９０３）に対し、一つの署名情報９０１が生成される場合の電子文書４１１の構成例を示している。また、図９（ｂ）は、署名情報９０１の詳細な構成例を示している。図９（ｂ）では、被署名データ１の識別情報９０５及び被署名データ２の識別情報９０７は、前述のステップＳ８０２で生成される。また、被署名データ１のダイジェスト値９０６及び被署名データ２のダイジェスト値９０８は、前述のステップＳ８０１で生成される。そして、９０５から９０８、即ち集約データ９０９を用いて、ステップＳ８０４において署名値９０４が生成される。

【００５９】
続いて、署名データ付加工程４０８について図７（ａ）を参照して説明する。７０１及び７０２は、中間電子文書生成工程４０５で生成された中間電子文書の伝達情報であり、７０３は、文書情報である。また７０４及び７０５は、署名情報生成工程４０７で生成された署名情報である。

【００６０】
署名情報には識別情報が埋め込まれており、この識別情報は、前述したように被署名データにあたる伝達情報や文書情報を指し示す。図７（ａ）においては署名情報７０４には被署名データ（即ち、伝達情報７０１）を指し示す識別情報７０６を埋め込む。署名情報と被署名データは一対一対応でなくてもよく、例えば、署名情報７０５には被署名データの伝達情報７０２及び文書情報７０３を指し示す識別情報７０７及び７０８を埋め込んでもよい。

【００６１】
ここで、伝達情報ａ（７０１）を、被署名データ１（９０２）と考え、伝達情報ｂ（７０２）及び文書情報７０３を被署名データ２（９０３）と考える。また、署名情報１（７０４）及び署名情報２（７０５）を、署名情報９０１と考えることができる。

【００６２】
次に、電子文書アーカイブ工程４０９について図７を参照して説明する。これまでの工程で生成された中間電子文書および署名情報は図７（ａ）のようにそれぞれが独立した個々のデータとして存在している。そこで、電子文書生成工程ではこれらのデータをひとつにアーカイブし電子文書を生成する。図７（ｂ）は中間電子文書と署名情報とをアーカイブ化した一例を示す模式図であり、アーカイブデータ７０９は図４の電子文書４１１に該当する。また図７（ａ）に記載の７０１から７０５については、７０１が７１３、７０２が７１４、７０３が７１２、７０４が７１０、そして７０５が７１１にそれぞれ対応する。

【００６３】
以上、本実施形態における電子文書生成工程について説明した。このように、本実施形態に対応する電子文書生成工程では、後々分離して再配布・再利用を行うことを想定してオリジナルコンテンツを複数のサブコンテンツに分離し、それぞれまたはそれらの組ごとに識別情報を与える。識別情報はステップＳ８０２の説明で前述したように、ＲＦＣ２３９６で規定されているＵＲＩを適用することもできる。これに限らず、例えば、オリジナルコンテンツにおけるサブコンテンツの相対的な位置情報を利用してもよい。また、サブ

コンテンツのヘッダ部分に一意に割り当てられた番号情報、ヘッダ部分に含まれるコンテンツホルダーや日時などの書誌情報、その他のメタデータから一方向性ハッシュ関数を用いて算出された値等を識別情報として用いてもよい。

【００６４】

更に、識別情報ごとにその識別情報に対応するサブコンテンツを入力とした一方向性ハッシュ関数の演算を行ってダイジェスト値を生成する。そして、識別情報およびダイジェスト値の組（集約データ）を複合コンテンツに付与する。これにより、文書操作工程において、オリジナルコンテンツから一部のサブコンテンツが削除され、残りのサブコンテンツのみで再構成されたコンテンツが流通している場合でも、再構成されたコンテンツの署名検証が可能となる。さらに、サブコンテツごとに署名を生成しなくても（つまり、サブコンテンツと１対１に対応させて署名を生成しなくても）、サブコンテンツごとに改竄されているかを検証可能となる。

【００６５】

再構成されたコンテンツにおける検証可能性については、以下で電子文書操作工程と関連させて説明する。

【００６６】

[電子文書操作工程]

図４の電子文書受信工程４１２にて受信された電子文書４１１は、電子文書展開工程４１３において電子文書アーカイブ工程４０９と逆の処理が施される。即ち、電子文書４１１が中間電子文書および署名情報の個々のデータに展開される。

【００６７】

署名情報検証工程４１５については、図１４（ｂ）で示した署名検証処理フローにおける入力データ：Ｍ（２１０７）が、集約データ９０９に相当する。同じくデジタル署名データ：Ｓ（２１１０）が署名情報９０１に、公開鍵２１１１は図４の公開鍵４１４に対応する。これにより、集約データ９０９に対する改竄の有無を判定することができる。

【００６８】

ここで集約データが改竄されていないことを確認できれば、集約データに含まれる識別情報に対応するダイジェスト値と、被署名データから生成されるダイジェスト値とが合致するかどうかの検証を行うことができる。以上の処理を、図９及び図１０を参照して以下に説明する。図１０は本実施形態に対応する署名検証処理の一例を示すフローチャートである。

【００６９】

図１０において、ステップＳ１００１では、電子文書展開工程４１３により電子文書４１１内の署名情報９０１を抽出する。次に、ステップＳ１００２では、図１４（ｂ）に記載の方法に基づき、署名情報９０１に含まれる署名値９０４に基づき、集約データ９０９の改竄が行われていないかどうかを検証する。即ち、識別情報９０５及びダイジェスト値９０６、識別情報９０７及びダイジェスト値９０８を入力データMとして、ダイジェスト値２１０９を生成する。更に、署名値９０４を公開鍵４１４を用いて復号し、ダイジェスト値を生成する。それぞれ生成されたダイジェスト値が一致するか否かを判定し、これが一致すれば、集約データ９０９には改竄が行われていないことが分かる。

【００７０】

次に、ステップＳ１００２において検証に失敗した場合には（ステップＳ１００２において「ＮＧ」）、署名検証処理を終え、結果としてＮＧを返却する。一方、ステップＳ１００２における検証に成功した場合には（ステップＳ１００２において「ＯＫ」）、ステップＳ１００３からＳ１００８における処理を、集約データ９０９に含まれる識別情報９０５及び９０７ごとに実行する。

【００７１】

次に、ステップＳ１００４では、識別情報に基づいて被署名データ９０２又は９０３を電子文書４１１中から取得する。ステップＳ１００５では、被署名データ９０２又は９０３を取得できたか否かをチェックし、取得できた場合にはステップＳ１００６に進む。取

得できなかった場合にはステップＳ１００８の処理に進み、もし次の識別情報が存在する場合には、対応する被署名データに対してステップＳ１００４の処理を行う。なお、電子文書４１１中から取得できない被署名データが存在する場合は、当該識別情報に対応するサブコンテンツが検証対象データとして含まれない旨を電子文書操作装置２０５に表示してもよい。この表示は、図１の構成では、例えばコンピュータ装置１０３や印刷装置１０４が備えるディスプレイ装置を利用して行うことができる。

【００７２】

ステップＳ１００６では、図１４（ｂ）に示す方法に基づいて被署名データ９０２又は９０３のダイジェスト値：Ｈ（Ｍ）を計算する。続くステップＳ１００７では、ダイジェスト演算結果と集約データ９０９に含まれているダイジェスト値９０６又は９０８と一致するか否かの判定を行う。両値が一致した場合には、ステップＳ１００８に進む。ステップＳ１００８では、次の識別情報が存在する場合には、対応する被署名データに対してステップＳ１００４の処理を行う。一致しなかった場合には、署名検証処理を終え、結果としてＮＧを返却する。ステップＳ１００８にてすべての識別情報に対して繰り返し処理を終えた場合には署名検証処理を終え、結果としてＯＫを返却する。

【００７３】

次に、図４の電子文書操作工程４１６について説明する。操作には閲覧、印刷などのコンテンツ消費処理が含まれるが、ユーザがコンテンツを享受する処理であればどのように消費されても本実施形態には影響しないため詳細を割愛する。一方、コンテンツ再構成処理は新たな電子文書４１１を再構成する処理であり、再構成された電子文書４１１は電子文書操作工程４０２に入力されることが想定される。

【００７４】

再構成された電子文書４１１は、電子文書生成工程４０１にて生成された電子文書４１１ではないため、署名情報にはアーカイブされていないコンテンツのダイジェスト値が含まれている場合がある。

【００７５】

そこで、図１１を参照して、再構成された電子文書４１１の検証について説明する。ここでは、例として、図９に示す電子文書４１１を受領したユーザが再構成処理を行い、被署名データ１（９０２）を削除して被署名データ２（９０３）のみをコンテンツとして配布する状況を想定する。

【００７６】

このとき配布される電子文書４１１は、図１１に示すように、書き換えられることとなる。即ち、電子文書４１１は署名情報９０１及び被署名データ２(９０３)で構成される。このとき、例えば、本来は署名検証時に不要なデータである９０５および９０６を冗長性排除のために削除する等して、署名情報９０１に手を加えれば、署名値９０４自体が無効となってしまう。従って、署名情報９０１すなわち９０４から９０８の情報は、再構成前の情報がそのまま使用されることになる。

【００７７】

ここで、図１０のフローチャートに基づいて処理を行った場合を考える。ステップＳ１００５では、被署名データ１の識別情報９０５に基づいて被署名データ１（９０２）の取得を試みるが、図１１の電子文書４１１にはアーカイブされていないため、取得できない。従って、ステップＳ１００５では「ＮＯ」の判定となって、ステップＳ１００８に移行し、次の識別情報（ここでは、識別情報９０７）について、ステップＳ１００４からの処理を継続する。このようにして、被署名データ１（９０２）については、ステップＳ１００７のダイジェストマッチング処理がスキップされる。一方、被署名データ２（９０３）は、ステップＳ１００４において受信され、ダイジェストマッチング処理が可能である。よって、被署名データ２（９０３）については、改竄の有無を検証することができる。

【００７８】

このように、集約データ９０９に記載されているが電子文書４１１内にアーカイブされていないサブコンテンツについてはダイジェストマッチング処理をスキップする。これに

より、アーカイブされているサブコンテンツについて、非改竄性を保証する仕組みを提供することができる。

【００７９】

従来の署名生成処理では、上記のように被署名データ１と被署名データ２のそれぞれに署名値を持たせる必要があった。従って、演算処理の負担が大きくなる。特に、分割された被署名データの分割数に比例して計算量が増加することになる。

【００８０】

これに対して、本実施形態では、コンテンツの分割回数に係わらず、署名値の演算処理を１回で済ませることができる。これにより、本実施形態では、従来よりも遙かに効率的に署名生成及び署名検証処理が可能となる。また、一部のサブコンテンツのみを使用して、データが再構成された場合であっても、該サブコンテンツが改竄されていないかどうかを確実に検証することができる。

【００８１】

以上説明したように、本発明によれば、テキストデータだけではなく多様なフォーマットで格納されたデジタルデータの複合体に対して、その一部分であるサブコンテンツが分離されて存在しても署名検証が可能となる。かつ、効率的に署名生成および署名検証処理が可能となる。　＜第２の実施形態＞

上記第１の実施形態の図１０に記載される検証処理では、サブコンテンツの一部が改竄されているがそれ以外は改竄性が認められない場合に、ユーザがコンテンツを許容する場合を考慮していない。そこで、本実施形態ではこの状況にも対応可能な方式について説明する。

【００８２】

図１０のステップＳ１００７では、ステップＳ１００６における演算結果として得られたダイジェスト値と、集約データ９０９に含まれているダイジェスト値とが一致しないサブコンテンツが発見された時点で、署名検証処理を終えることとしている。しかしながら、このような場合であっても両ダイジェスト値が一致する、或いは、未処理の他のサブコンテンツが存在し、被署名データの非改竄性が保証される可能性のある場合には、署名検証処理を継続してもよい。

【００８３】

そこで、本実施形態では、ステップＳ１００７のマッチング結果がＮＧの場合でも強制的に処理を終了せず、集約データ９０９に含まれる他の識別情報のすべてについてステップＳ１００３からＳ１００８の検証処理を継続する。そして、検証結果として、非改竄性が認められるサブコンテンツと、改竄されているサブコンテンツのそれぞれのリストを返却する。これにより、改竄の有無に関する情報を、サブコンテンツ単位に、コンピュータ装置１０３や印刷装置１０４などを介してユーザに通知することができる。

【００８４】

このようにすれば、一部のサブコンテンツが改竄されているが、他のサブコンテンツは改竄性が認められない場合にコンテンツを許容することができる。これにより、改竄されていないサブコンテンツについては、再利用を可能とする仕組みを提供できる。

【００８５】

＜第３の実施形態＞

本実施形態では、被署名データのユーザによる選択を可能とする場合を説明する。上述の実施形態では署名情報生成工程４０７において署名処理が行われ、その詳細な処理は図８に記載した通りである。図８では、電子化された文書データの全体が被署名データとして処理され、文書データのいずれかの領域のみを選択して署名処理を行うものではなかった。

【００８６】

そこで本実施形態では、中間電子文書工程４０５と署名情報生成工程４０７との間に、被署名データを選択する工程を新たに設けることを特徴とする。この工程のことを、本実施形態では、被署名データ選択工程と呼ぶこととする。以下、被署名データ選択工程につ

いて説明する。

【００８７】

被署名データ選択工程では、紙文書入力工程４０４でスキャンされた画像データが、装置の画面上に図６（ａ）のような形態で表示される。その際、ユーザは被署名データをマウスなどのデバイスポインタを用いて矩形領域の指定を行うことができる。例えば、「１９０１年に連邦制国家が成立し・・・めぐる旅です。」と記載された領域をデバイスポインタにより指定することができる。

【００８８】

また、図６（ｂ）のような形態で表示が行われる場合には、デバイスポインタにより各矩形情報（６０２から６０６）のいくつかを選択することができる。このような矩形情報は、既に内部で保持しているデータ構造として扱いやすい分割単位であるため、係る矩形情報の選択は直後に行われる署名情報生成工程４０７に即した処理といえる。

【００８９】

図１２は図６（ｂ）のうち、２つの分割領域（６０２および６０６）が被署名データとして選択された例を示す。図１２では、選択した分割領域が強調されており、ユーザが選択された領域を識別しやすい画面構成となっている。

【００９０】

これに対し、ユーザは中間電子文書工程４０５で分割された領域よりも更に狭い領域に対して署名を行うことを希望することもありえる。例えば、サブコンテンツとして今後分割される可能性が高いと思われる領域が、中間電子文書工程４０５で分割された領域よりも更に狭い領域である場合が考えられる。

【００９１】

このような場合を想定し、本実施形態におけるユーザインタフェースでは、図１３に示すように分割領域を更に細かい領域に分割可能であることが望ましい。この例では、領域６０６よりもさらに狭い領域１３０１が選択され強調されていることがわかる。

【００９２】

なお、このような更に狭い領域の指定を可能とする場合には、中間電子文書工程４０５のステップＳ５０２において領域分割を行う際に、ユーザから所望の領域（例えば、図１３における領域１３０１）の指定を受け付けることができる。指定の受付は、ユーザが希望する領域をデバイスポインタにより指定し、これを受け付けることにより行うことができ、係る技術は公知であるので、本明細書における詳細な説明は省略する。

【００９３】

このように中間電子文書工程４０５で定められた分割よりも更に細かい分割を行い、署名情報生成工程４０７において被署名データとして利用することが可能となれば、ユーザにとってより自由度の高い被署名データの選択方法となる。

【００９４】

なお、ここで、領域１３０１を分割領域のひとつとしてもよいし、領域６０６と領域１３０１との差分情報を新たな分割領域としても構わない。前者の場合、電子文書４１１のデータ量が増えるが処理が容易であり、後者の場合、新たな領域分割を行うための処理が必要となる。

【００９５】

以上によれば、ユーザは、被署名データを選択して、署名情報生成処理を行うことができる。また、予め分割された矩形領域に限らず、任意の領域を指定して被署名データとすることができる。

【００９６】

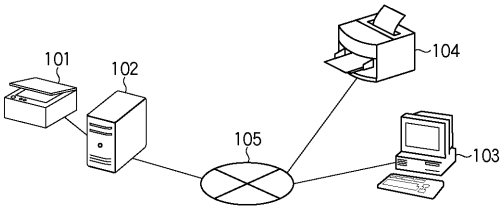
＜他の暗号アルゴリズムによる実施形態＞

前述の実施形態では公開鍵暗号方式による暗号処理（秘匿化）方法を示した。しかし、共通鍵暗号方式による暗号処理方法およびＭＡＣ（メッセージ認証子）生成方法への適用は容易であり、他の暗号アルゴリズムを適用することによって上記実施の形態が実現される場合も本発明の範疇に含まれる。

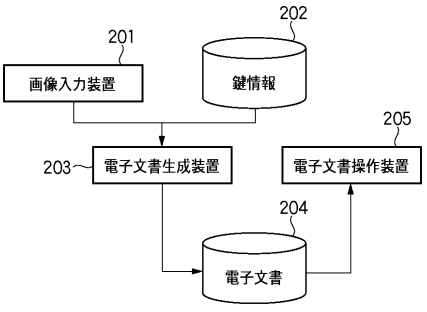
【００９７】
＜ソフトウエアなどによる他の実施の形態＞
なお、本発明は、複数の機器（例えばホストコンピュータ、インタフェイス機器、リーダ、プリンタなど）から構成されるシステムに適用しても、一つの機器からなる装置（例えば、複写機、ファクシミリ装置など）に適用してもよい。
【００９８】
また、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体（または記録媒体）を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。
【００９９】
この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。
【０１００】
さらに、フロッピーディスク（登録商標）、ハードディスク、光ディスク、磁気光ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、磁気タイプや不揮発性タイプのメモリーカード及びＲＯＭのような記憶媒体を当該プログラムコードを提供するために利用することができる。
【０１０１】
また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているオペレーティングシステム（ＯＳ）などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。
【０１０２】
さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張カードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張カードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。
【０１０３】
本発明が上述の記憶媒体について適用される場合、当該記憶媒体は上記実施形態において記載されたフローチャートに対応するプログラムコードを格納することが好ましい。その一方、本発明は上述の実施形態に限定されることなく、本発明の精神及び範囲において様々な変更や修正を加えることが可能である。それゆえに、本発明の範囲を公に知らしめるべく以下の特許請求の範囲が作成される。
【０１０４】
このように、本発明の動作及び構成は上述の記載から明らかとなるものと信ずる。開示及び記述された方法、装置及びシステムは好適に特徴づけられる一方、以下の特許請求の範囲において定義される本発明の範囲から逸脱することなく様々な変更及び修正が可能であることは、直ちに明らかとなるであろう。
【図面の簡単な説明】
【０１０５】
【図１】本発明の実施形態に対応するシステムの構成の一例を示す図である。
【図２】本発明の実施形態に対応するシステムの機能構成の一例を示す図である。
【図３】本発明の実施形態に対応するハードウエア構成の一例を示す図である。
【図４】本発明の実施形態に対応する電子文書生成工程及び電子文書操作工程の機能ブロック図である。
【図５】本発明の実施形態に対応する中間電子文書生成工程における処理の一例を示すフ

ローチャートである。
【図６】本発明の実施形態に対応する電子データの一例を説明する図である。
【図７】本発明の実施形態に対応する中間電子文書及び電子文書を説明するための図である。
【図８】本発明の実施形態に対応する署名生成工程における処理の一例を示すフローチャートである。
【図９】本発明の実施形態に対応する電子文書の構成の一例を示す図である。
【図１０】本発明の実施形態に対応する署名検証工程の処理の一例を示すフローチャートである。
【図１１】本発明の実施形態に対応する再構成処理後の署名データの構成の一例を示す図である。
【図１２】本発明の第３の実施形態に対応する電子データの閲覧例を説明するための図である。
【図１３】本発明の第３の実施形態に対応する電子データの他の閲覧例を説明するための図である。
【図１４】署名作成処理及び署名検証処理の一般例を表す模式図である。
【図１５】公開鍵証明書X.５０９v.３のデータフォーマットを説明するための図である。

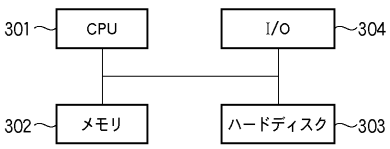
【図１】



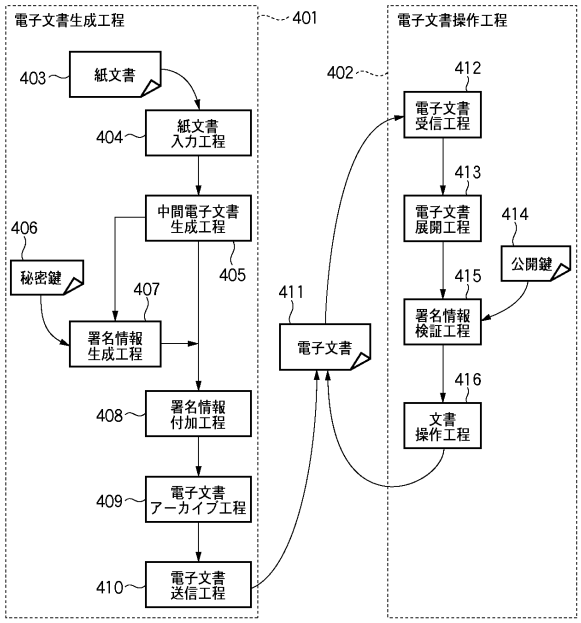
【図２】



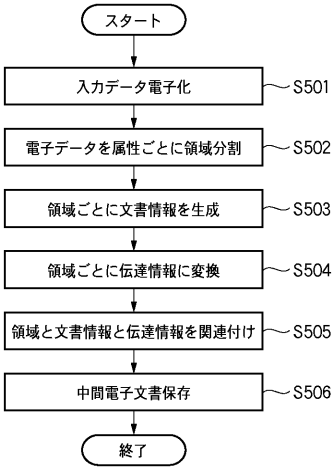
【図３】



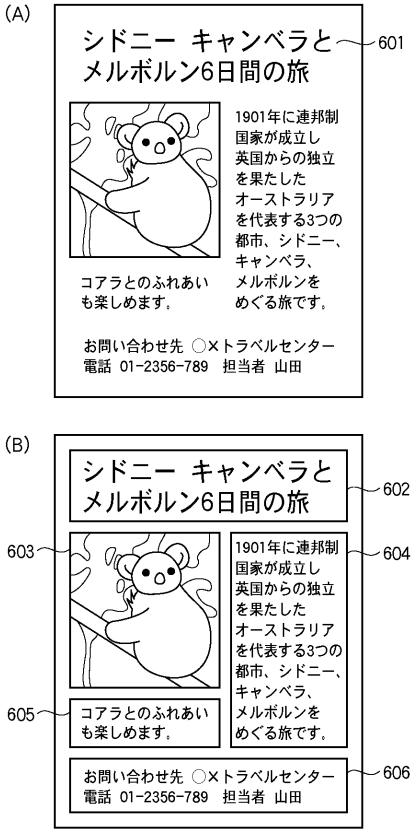
【図４】



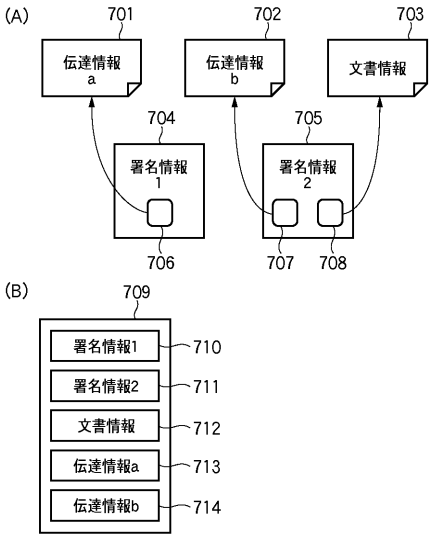
【図５】


スタート
入力データ電子化
S501
電子データを属性ごとに領域分割
S502
領域ごとに文書情報を生成
S503
領域ごとに伝達情報に変換
S504
領域と文書情報と伝達情報を関連付け
S505
中間電子文書保存
S506
終了

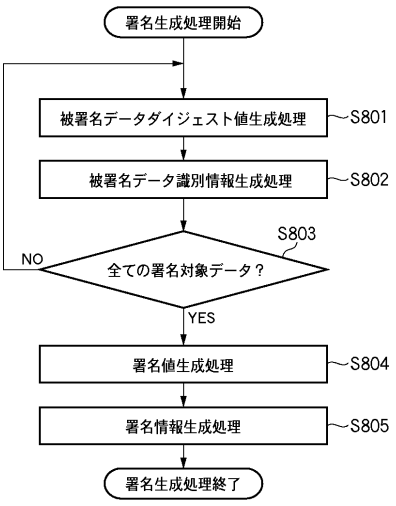
【図６】


(A)
シドニー キャンベラと
メルボルン6日間の旅
601
1901年に連邦制
国家が成立し
英国からの独立
を果たした
オーストラリア
を代表する3つの
都市、シドニー、
キャンベラ、
メルボルンを
めぐる旅です。
コアラとのふれあい
も楽しめます。
お問い合わせ先 ○×トラベルセンター
電話 01-2356-789 担当者 山田
(B)
シドニー キャンベラと
メルボルン6日間の旅
602
603
1901年に連邦制
国家が成立し
英国からの独立
を果たした
オーストラリア
を代表する3つの
都市、シドニー、
キャンベラ、
メルボルンを
めぐる旅です。
604
605
コアラとのふれあい
も楽しめます。
お問い合わせ先 ○×トラベルセンター
電話 01-2356-789 担当者 山田
606

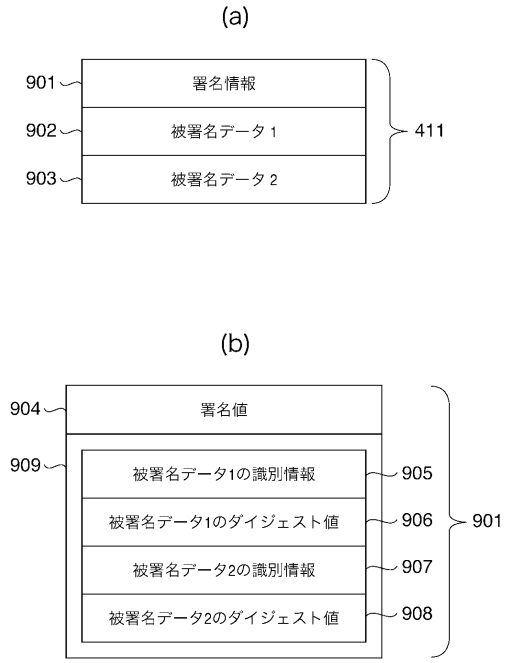
【図７】


(A)
701
伝達情報
a
702
伝達情報
b
703
文書情報
704
署名情報
1
705
署名情報
2
706
707
708
(B)
709
署名情報1
710
署名情報2
711
文書情報
712
伝達情報a
713
伝達情報b
714

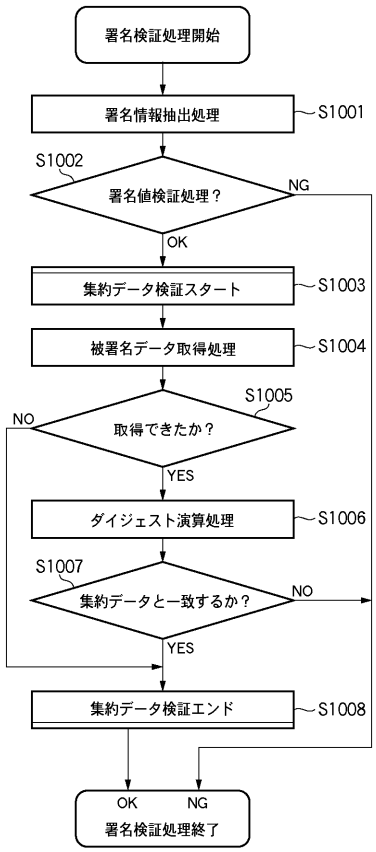
【図８】


署名生成処理開始
被署名データダイジェスト値生成処理
S801
被署名データ識別情報生成処理
S802
S803
NO
全ての署名対象データ？
YES
署名値生成処理
S804
署名情報生成処理
S805
署名生成処理終了

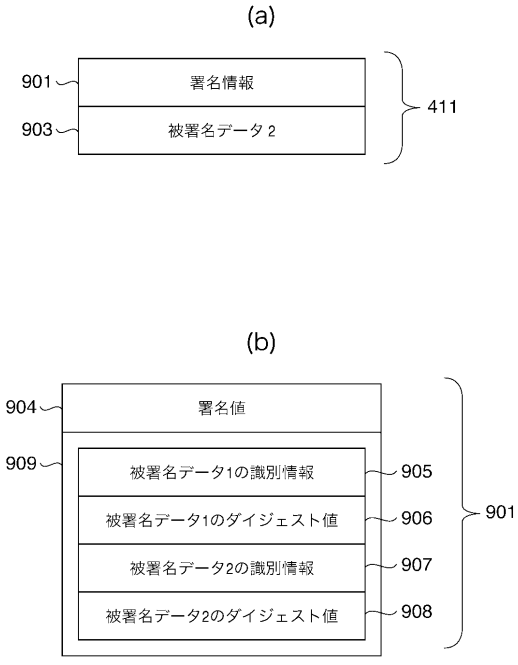
【図９】



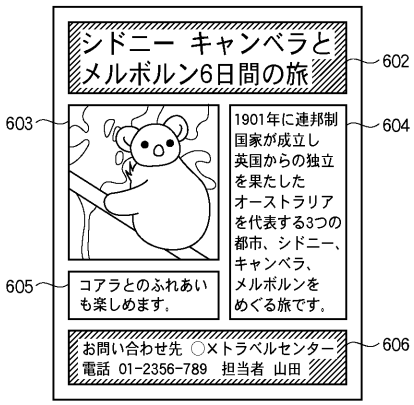
【図１０】



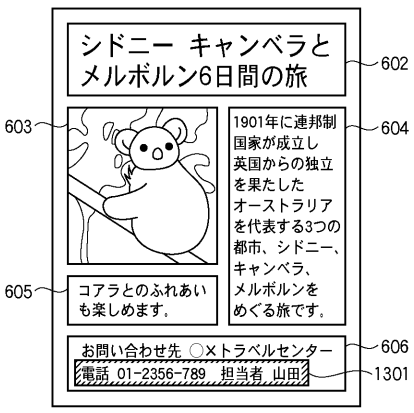
【図１１】



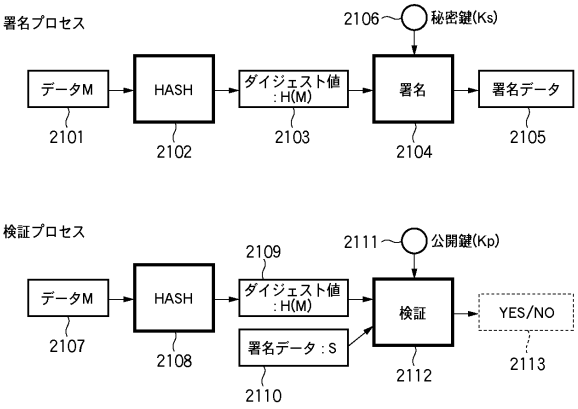
【図１２】



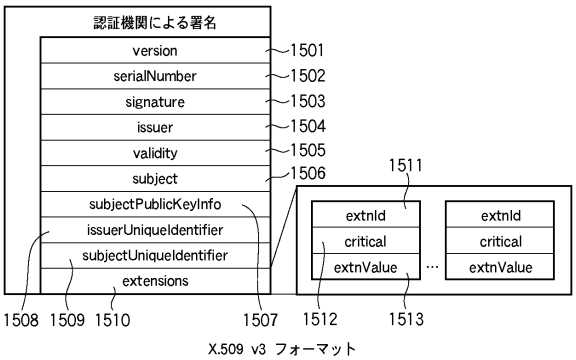
【図１３】



【図１４】


署名プロセス
2106
秘密鍵(Ks)
データM
HASH
ダイジェスト値
:H(M)
署名
署名データ
2101
2102
2103
2104
2105
検証プロセス
2109
2111
公開鍵(Kp)
データM
HASH
ダイジェスト値
:H(M)
検証
YES/NO
署名データ:S
2107
2108
2110
2112
2113

【図１５】


認証機関による署名
version
serialNumber
signature
issuer
validity
subject
subjectPublicKeyInfo
issuerUniqueIdentifier
subjectUniqueIdentifier
extensions
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
extnId
critical
extnValue
1512
1513
X.509 v3 フォーマット

フロントページの続き

審査官　松平　英

(56)参考文献　特開２００５－０５１７３４（ＪＰ，Ａ）
特開平０６－２２４８９６（ＪＰ，Ａ）
特開平１０－００３２５７（ＪＰ，Ａ）
特開平１０－３２６０７８（ＪＰ，Ａ）
特開２００１－２２３７３５（ＪＰ，Ａ）
特開２００２－３３３８３５（ＪＰ，Ａ）
特開２００４－３６４０７０（ＪＰ，Ａ）
特開２００６－０６０７７２（ＪＰ，Ａ）
特開２００６－１８０４７２（ＪＰ，Ａ）
特開２００７－０６０５９４（ＪＰ，Ａ）
特開２００７－０８１４５１（ＪＰ，Ａ）
特開２００７－０８１４５２（ＪＰ，Ａ）
特開２００７－０８１４８２（ＪＰ，Ａ）
特開２００７－１０２７５７（ＪＰ，Ａ）
国際公開第２００８／０１５７４０（WO，Ａ１）
国際公開第２００８／０１５７５５（WO，Ａ１）
宮崎　邦彦　他，電子文書黒塗り問題，情報処理学会研究報告，日本，社団法人情報処理学会，２００３年　7月１８日，Ｖｏｌ．２００３　Ｎｏ．７４，ｐ．６１～６７
増渕　孝延　他，内部不正者を考慮した墨塗り箇所変更可能方式の提案，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，２００５年　7月１４日，Ｖｏｌ．１０５　Ｎｏ．１９２，ｐ．１７９～１８６

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／００
Ｇ０９Ｃ　　１／００
Ｇ０６Ｆ　２１／２０
Ｇ０６Ｑ　５０／００