(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-51734
(P2005-51734A)
(43)公開日　平成17年2月24日(2005.2.24)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 9/32	H04L 9/00	675B	5B017
G06F 12/14	G06F 12/14	310Z	5J104

審査請求 未請求　請求項の数 15　ＯＬ　（全 27 頁）

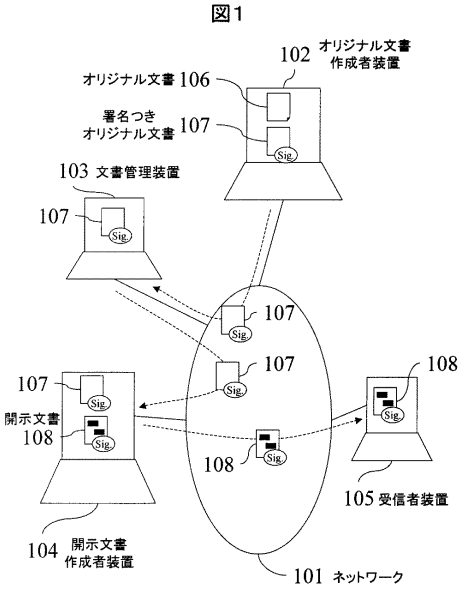
(21)出願番号　特願2004-7458(P2004-7458)
(22)出願日　平成16年1月15日(2004.1.15)
(31)優先権主張番号　特願2003-196860(P2003-196860)
(32)優先日　平成15年7月15日(2003.7.15)
(33)優先権主張国　日本国(JP)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100075096
弁理士　作田　康夫
(74)代理人　100100310
弁理士　井上　学
(72)発明者　宮崎　邦彦
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
(72)発明者　岩村　充
東京都練馬区中村２－１４－１７
(72)発明者　松本　勉
神奈川県横浜市青葉区柿の木台１３－４５
最終頁に続く

(54)【発明の名称】電子文書の真正性保証方法および電子文書の公開システム

(57)【要約】
【課題】
開示文書の真正性の保証と、開示不適当な情報の削除の両立可能な、電子文書の真正性保証技術、および情報公開システムが求められる。
【解決手段】
電子文書を構成要素に分割し、その構成要素全体からなる集合の任意の部分集合に対し署名を付与する。または、その構成要素おのおのと、該各構成要素と該電子文書の構造との関係を規定する情報とを結合したデータに対し、署名を付与する。または、その構成要素おのおのに対しハッシュ値を計算し、計算されたハッシュ値を結合したデータに対し署名を付与する。または、その構成要素おのおのに対して生成した乱数を結合し、乱数が結合された構成要素に対し、ハッシュ値を計算し、計算されたハッシュ値を結合したデータに対し電子署名を付与する。
【選択図】　図１

図1



【特許請求の範囲】
【請求項１】
電子文書の真正性保証方法であって、
電子文書を複数の構成要素に分割し、
前記複数の構成要素からなる集合の、すべての部分集合に対して、電子署名を付与する。
【請求項２】
電子文書の真正性保証方法であって、
電子文書を複数の構成要素に分割し、
前記複数の構成要素おのおのに、当該構成要素と該電子文書の構造との関係を規定する情報を結合したデータを作成し、
前記結合したデータに対し、電子署名を付与する。
【請求項３】
電子文書の真正性保証方法であって、
電子文書を複数の構成要素に分割し、
前記複数の構成要素おのおのと、当該構成要素について暗号学的ハッシュ関数を用いて計算したハッシュ値を結合したデータを作成し、
前記結合データに対し電子署名を付与する。
【請求項４】
電子文書の真正性保証方法であって、
電子文書を複数の構成要素に分割し、
前記複数の構成要素おのおのに、乱数を生成して結合し、
前記乱数が結合された複数の構成要素おのおのと、乱数が結合された当該構成要素について暗号学的ハッシュ関数を用いて計算したハッシュ値を結合したデータを作成し、
前記結合データに対し電子署名を付与する。
【請求項５】
電子文書の公開システムであって、
オリジナル文書作成者装置において、
電子文書を複数の構成要素に分割し、
前記複数の構成要素からなる集合の、すべての部分集合に対して、電子署名を付与し、文書管理装置に格納しておき、
開示文書作成者装置において、
情報公開請求受け付け時に、文書管理装置内の電子文書から開示対象文書を取り出し、該開示対象文書に含まれる開示すべきでない情報を取り除いた開示文書を作成し、受信者装置に送り、
受信者装置において、
公開された開示文書受信時に、オリジナル文書作成者の署名を検証する。
【請求項６】
第三者機関装置を利用した電子文書の真正性保証方法であって、
電子文書を複数の構成要素に分割し、
前記複数の構成要素からなる集合の、すべての部分集合を、保証対象情報として第三者機関装置に預託する。
【請求項７】
電子文書の真正性保証方法であって、
電子文書を複数の構成要素に分割し、
前記複数の構成要素おのおのに、当該構成要素と該電子文書の構造との関係を規定する情報を結合したデータを作成し、
前記結合したデータを保証対象情報として第三者機関装置に預託する。
【請求項８】
電子文書の真正性保証方法であって、

電子文書を構成要素に分割し、
その構成要素おのおのに対し暗号学的ハッシュ関数を用いてハッシュ値を計算し、計算されたハッシュ値を結合したデータを、保証対象情報として第三者機関装置に預託する。
【請求項９】
電子文書の真正性保証方法であって、
電子文書を構成要素に分割し、
その構成要素おのおのに、乱数を生成して結合し、乱数が結合された構成要素に対し、暗号学的ハッシュ関数を用いてハッシュ値を計算し、計算されたハッシュ値を結合したデータを、保証対象情報として第三者機関装置に預託する。
【請求項１０】
電子文書の公開システムであって、
オリジナル文書作成者装置において、作成した電子文書に対して、請求項６から請求項９のいずれかひとつに記載の、第三者機関装置を利用した電子文書の真正性保証方法に従って第三者機関装置に保証対象情報を預託し、また前記保証対象情報を文書管理装置に格納しておき、
開示文書作成者装置において、
情報公開請求受け付け時に、文書管理装置内の電子文書から開示対象文書を取り出し、該開示対象文書に含まれる開示すべきでない情報を取り除いた開示文書を作成し、受信者装置に送り、
受信者装置において、
公開された開示文書受信時に、前記第三者機関装置に前記開示文書の真正性検証を要求する。
【請求項１１】
請求項１から請求項４のいずれかひとつに記載の電子文書の真正性保証方法に従って、電子署名を付与された電子文書の開示方法であって、
前記電子署名を付与された前記電子文書を開示対象文書とし、
前記開示対象文書に含まれる開示すべきでない情報を取り除いた開示文書を作成し、
開示文書に対して、さらに署名を付与する。
【請求項１２】
請求項５記載の電子文書の公開システムであって、
前記開示文書作成者装置において、
開示すべきでない情報を取り除いた前記開示文書に対し、開示文書作成者装置の他の署名を付与する。
【請求項１３】
電子文書の真正性保証方法であって、
電子文書を複数の構成要素に分割し、
前記複数の構成要素おのおのに対応する非開示を示すデータを作成し、
前記各構成要素と、当該構成要素に対応する非開示を示すデータとから、当該構成要素に関する署名対象データを計算し、
計算した前記署名対象データを結合し、
前記結合データに対し電子署名を付与する。
【請求項１４】
電子文書の開示方法であって、
請求項１３記載の電子文書の真正性保証方法に従って作成された署名付き電子文書を構成する各構成要素に対し、
開示すべきでない第一の情報を含む場合には、当該第一の情報に対応する構成要素は取り除き、当該第一の情報に対応する非開示を示すデータを残し、
開示すべきで、かつ、将来的に非開示とされるべきでない第二の情報を含む場合には、当該第二の情報に対応する構成要素は残し、当該第二の情報に対応する非開示を示すデータは取り除き、

開示すべきで、かつ、将来的に非開示とされうる第三の情報を含む場合には、当該第三の情報に対応する構成要素と非開示を示すデータとの両方を残す。
【請求項１５】
電子文書の公開システムであって、
オリジナル文書作成者装置において、作成した電子文書に対して、請求項１３に記載の電子文書の真正性保証方法に従って、電子署名を付与し、文書管理装置に格納しておき、
開示文書作成者装置において、
情報公開請求受け付け時に、文書管理装置内の電子文書から開示対象文書を取り出し、該開示対象文書に含まれる各構成要素に対し、
開示すべきでない第一の情報を含む場合には、当該第一の情報に対応する構成要素は取り除き、当該第一の情報に対応する非開示を示すデータを残し、
開示すべきで、かつ、将来的に非開示とされるべきでない第二の情報を含む場合には、当該第二の情報に対応する構成要素は残し、当該第二の情報に対応する非開示を示すデータは取り除き、
開示すべきで、かつ、将来的に非開示とされうる第三の情報を含む場合には、当該第三の情報に対応する構成要素と非開示を示すデータとの両方を残した、
開示文書を作成し、受信者装置に送り、
前記受信者装置において、
公開された開示文書受信時に、前記オリジナル文書作成者の署名を検証する。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、電子データの真正性保証技術に関する。
【背景技術】
【０００２】
従来、電子文書等の電子データの真正性保証を行う技術として、電子署名（ディジタル署名ともいう）技術がある。（例えば、非特許文献１参照）。
【０００３】
また、構造化された電子文書の各エンティティを電子署名つきで参照・編集可能な構造化文書として取り出す技術がある。（例えば、特許文献１参照）。
【０００４】
また、所有者とは異なる署名者によってあらかじめ署名が付与された所有者(owner)が所有する文書から、署名者が許可した部分については削除可能であり、また削除したあとの署名付き文書の有効性が確認可能な技術がある。（例えば、非特許文献２参照）。
【０００５】
【非特許文献１】Bruce Schneier著「Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition」 John Wiley & Sons、(October 18, 1995), pp. 483-502.
【０００６】
【非特許文献２】Ron Steinfeld, Laurence Bull, Yuliang Zheng著,”Content Extraction Signatures", In International Conference on Information Security and Cryptology ICISC 2001, volume 2288 of LNCS, pp. 285-304, Berlin, 2001. Springer-Verlag, (2001)
【特許文献１】特開2001-167086号公報(第17図)
【発明の開示】
【発明が解決しようとする課題】
【０００７】
電子文書の安全性を支える重要な技術である現在の電子署名技術は、電子文書に対する１ビットの改変であっても検知できるように設計されている。この性質は、不正者による改ざんから電子文書を守るという意味では、非常に有用であるが、電子文書の有効活用と

いう観点からは、一切の加工が許されなくなるため、逆に障害となりうる。
【０００８】
この問題を端的に示す利用場面としては、行政機関等における情報公開が挙げられる。たとえば，次のような電子署名の利用形態が想定される。
【０００９】
すなわち、行政機関において、職員が職務上作成した文書（行政文書）は、作成者を明らかにし、また、改ざんを防止するために、電子署名を付された上で保管される。この文書が情報公開法に基づき開示されるときに、そこに記述された個人情報や国家安全情報が削除や墨塗りなどの処理により部分的に非公開にされた上で開示される。
【００１０】
従来の電子署名技術では、上記の一連の手続きに従って開示された文書の真正性、すなわち、文書作成者が誰であるか、また開示された文書はもともと作成された文書と同一であるか、を確認することができない。なぜなら、情報公開の過程で、文書の一部が削除されているからである。悪意による改ざんであろうと、プライバシー情報の保護のための個人情報削除であろうと、署名対象文書に対し、なんらかの改変が加えられた、という点では変わらない。結果として、従来の電子署名技術の利用では、「公開された文書の真正性保証」と、「プライバシー情報の保護」という２つの重要なセキュリティ要件を両立できず、どちらかをあきらめざるをえない。
【００１１】
情報公開制度が、行政機関のアカウンタビリティ（説明責任）を果たすための制度であるということを考えると、個人情報等が削除された後の開示用の文書からでも、元々の行政文書との同一性を検証できることが望ましい。
【００１２】
特許文献１に記載された技術では、電子文書の各エンティティのデータと、電子署名データとの対応付けについては開示しているが、電子文書編集後に、元の電子署名を変更することなく、元の文書の真正性を確認することについては、開示していない。
【００１３】
したがって、真正性保証対象文書に対する適切な改変を許容する電子文書の真正性保証技術、言い換えると電子文書編集後に、元の電子署名を変更することなく、元の文書の真正性を確認可能な技術が望まれている。
【００１４】
非特許文献２に記載された技術では、所有者(owner)が所有する、所有者とは異なる署名者によってあらかじめ署名が付与された文書から、署名者が許可した部分については削除可能であり、また削除したあとの署名付き文書の有効性が確認可能な技術が開示されているが、情報公開制度に適した技術は開示されていない。
【００１５】
例えば、情報公開の場合には、署名者とは異なる開示文書作成者が、署名者が作成または内容を確認したオリジナル文書の開示部分を決定し、開示不適当な部分については情報を削除し、開示すべき部分については、さらにその内容に応じて、第３者による更なる削除を許容または防止可能な状態で情報を開示することが望まれる。しかし、非特許文献２は、このような開示文書作成者が、第３者による再改変を許可または防止を選択可能な技術については開示していない。
【００１６】
したがって、真正性保証対象文書に対する適切な改変を施した文書の利用形態および要求される要件に合わせた情報公開方法および公開システムが望まれている。
【課題を解決するための手段】
【００１７】
本発明は、真正性保証対象文書に対する適切な改変を許容する電子文書の真正性保証技術と文書管理システムを提供する。
【００１８】

本発明は、その一態様において、電子文書を構成要素に分割し、その構成要素全体からなる集合の任意の部分集合に対し電子署名を付与する電子署名方法を提供する。

【００１９】

また、本発明は、他の一態様において、電子文書を構成要素に分割し、その構成要素おのおのと、該各構成要素と該電子文書の構造との関係を規定する情報とを結合したデータに対し、電子署名を付与する電子署名方法を提供する。

【００２０】

また、本発明は、他の一態様において、電子文書を構成要素に分割し、その構成要素おのおのに対し暗号学的ハッシュ関数を用いてハッシュ値を計算し、計算されたハッシュ値を結合したデータに対し電子署名を付与する電子署名方法を提供する。

【００２１】

また、本発明は、他の一態様において、電子文書を構成要素に分割し、その構成要素おのおのに、乱数を生成して結合し、乱数が結合された構成要素に対し、暗号学的ハッシュ関数を用いてハッシュ値を計算し、計算されたハッシュ値を結合したデータに対し電子署名を付与する電子署名方法を提供する。なお、ハッシュ関数とは、任意の長さのメッセージから、決まった（短い）長さのデータ（これをハッシュ値という）に変換する関数のことである。ハッシュ関数の中でも、特に、出力が、ある与えられたハッシュ値となる入力メッセージを見つけることが困難（一方向性という）であり、同じハッシュ値となる2つの異なる入力メッセージを見つけることが困難（衝突困難性という）である、という２つの性質を持つものを暗号学的ハッシュ関数と呼ぶ。

【００２２】

本発明の一態様によれば、行政機関等における情報公開において、オリジナル電子文書作成時に、オリジナル文書作成者が、作成した電子文書に対して、前記本発明の一態様によって提供される電子署名方法に従って、電子署名を付与し、文書管理装置に格納しておく。情報公開請求受け付け時に、開示文書作成者が文書管理装置内の電子文書から開示対象文書を取り出し、該開示対象文書に含まれる個人情報等の開示すべきでない情報を取り除いた開示文書を作成し、公開のために受信者装置に送り、公開された開示文書受信時に、受信者がオリジナル文書作成者の署名を検証可能な電子文書公開システムを提供する。

【発明の効果】

【００２３】

本発明によれば、部分情報を削除後であっても電子文書の真正性が検証可能な電子文書の真正性保証が提供される。また、個人情報等の重要情報の機密性と開示文書の真正性を保証可能な情報公開システムが提供される。

【発明を実施するための最良の形態】

【００２４】

図１は、本発明を、情報公開システムに適用した複数の実施形態におけるシステムの概略構成図である。なお、以下では、行政機関の情報公開システムを例に挙げているが、行政機関以外の組織や個人における情報公開システムであっても同様に適用可能である。

【００２５】

図示するように、本システムは、ネットワーク１０１を介して、情報公開側である行政機関の職員が利用する、オリジナル文書作成者装置１０２、文書管理装置１０３、開示文書作成者装置１０４の各装置と、情報公開の請求側と検証側である一般市民が利用する受信者装置１０５が接続されている。

【００２６】

なお、以下の各実施形態では、行政機関の職員が利用する、オリジナル文書作成者装置１０２、文書管理装置１０３、開示文書作成者装置１０４の各装置と、一般市民が利用する受信者装置１０５が、同一のネットワーク１０１に接続されている例を説明しているが、これとは異なる接続形態であってもよい。たとえば、行政機関の職員が利用する、オリジナル文書作成者装置１０２、文書管理装置１０３、開示文書作成者装置１０４の各装置が、当該行政機関のLAN(Local Area Network)に接続されており、当該LANが、ゲートウェ

イサーバを介して、一般市民が利用する受信者装置１０５が接続されているネットワーク１０１に接続されるようになっていてもよい。このような接続形態をとった場合、行政機関のLANは、ゲートウェイサーバにより、外部ネットワーク１０１からの不正アクセス等の攻撃から防御できることになるため、情報セキュリティの観点からは好ましい。

【００２７】

オリジナル文書作成者装置１０２は、行政機関の職員であるオリジナル文書作成者が、電子データとして行政文書（職務上作成する文書）を作成し、作成した行政文書に対し、電子署名を付与したのち、文書管理装置１０３に署名付き行政文書を要求するために利用される。以下の各形態の説明では、以降、オリジナル文書作成者が署名を付す対象とした行政文書のことを、オリジナル文書１０６と呼ぶ。なお、以下の各形態では、オリジナル文書の作成と、オリジナル文書１０６への署名の付与を、ともにオリジナル文書作成者装置において行う例を示すが、これとは異なり、オリジナル文書の作成とオリジナル文書への署名を行う装置とを分け、ネットワーク１０１や可搬な記憶媒体を用いて、これらの装置間でオリジナル文書１０６の受け渡しを行うようにしてもよい。

【００２８】

文書管理装置１０３は、オリジナル文書作成者装置１０２から要求を受けて、オリジナル文書作成者装置１０２で作成された署名付きオリジナル文書１０７を保管する。また、開示文書作成者装置１０４からの要求を受けて、あらかじめ保管していた開示対象となる署名付きオリジナル文書１０７を、開示文書作成者装置１０２に送信する。なお、オリジナル文書作成者装置１０２からの保管要求受付時と、開示文書作成者装置１０４からの開示対象文書送信要求受付時には、適切なユーザ認証処理等を行うことによって、アクセス制御を行うことが、情報セキュリティの観点からは好ましい。

【００２９】

開示文書作成者装置１０４は、受信者装置１０５の利用者である一般市民などの操作による情報公開請求を受けて、当該情報公開請求に応じた開示対象文書を検索し、当該開示対象文書である署名付きオリジナル文書１０７の送信を文書管理装置１０３に要求する。次に、開示文書作成者装置１０４の操作者の操作により、文書管理装置１０３から受信した署名付きオリジナル文書１０７に含まれる情報のうち、個人情報保護や、国家機密にかかわる情報の保護の観点から、公開に不適切な情報を取り除いた開示文書１０８を作成し、作成した開示文書を受信者装置１０５に対し公開する。

【００３０】

このとき、オリジナル文書１０６に付された署名が、従来の電子署名技術によって生成された署名である場合、「公開に不適切な情報の削除」であっても、オリジナル文書１０６に対する不正な改ざんがあった場合と同様に、署名検証の際に検証に失敗するという結果になってしまう。各実施形態では、不適切な情報削除後であっても検証可能な、あらたな電子署名技術を適用する。

【００３１】

公開する方法は、たとえば、電子メールで送信する、行政機関または他の機関が運用するWebサーバにアップロードするなど、任意に設計すればよい。Webサーバにアップロードする方法の場合は、情報公開請求を行った受信者装置１０５の利用者以外の一般市民であっても、公開された情報を閲覧できるというメリットがある。

【００３２】

なお、各実施形態では、一般市民からの情報公開請求受付、開示対象文書の検索、開示対象文書の文書管理装置１０３への要求、開示文書１０８の作成、開示文書１０８の公開を、同一の開示文書作成者装置１０５において行う例を示すが、これとは異なっていてもよい。たとえば、一般市民からの情報公開請求受付、開示対象文書の検索、開示対象文書の文書管理装置１０３への要求、を開示文書作成者装置１０５とは異なる、別の装置において行い、開示文書１０８の作成と開示文書１０８の公開を開示文書作成者装置１０５で行うようにしてもよい。

【００３３】

受信者装置１０５は、利用者である一般市民が、行政機関に対し情報公開請求を行い、その結果公開された開示文書１０８の真正性を検証するために利用される。受信者装置１０５は、開示文書作成装置１０４に対し、開示対象文書を特定するのに必要な情報を送信し、情報公開を請求する。また、公開された開示文書１０８とオリジナル文書１０６の内容とが、情報の保護の観点から取り除かれた部分（非開示部分）を除き、同一であるかどうかを検証する。

【００３４】

また、受信者装置１０５は、公開された開示文書１０８を、利用者が閲覧できるように、非開示部分が黒く塗りつぶされた（以下、墨塗りされたという）状態で表示または印刷を行う。

【００３５】

なお各実施形態では、情報公開請求と、開示文書１０８の真正性検証を、同一の受信者装置１０５で行う例を示すが、これとは異なっていてもよい。たとえば、情報公開請求を、受信者装置１０５とは別の装置で行い、その結果公開された開示文書１０８の真正性検証を、受信者装置１０５で行うようにしてもよい。

【００３６】

図２は、以下の各形態におけるオリジナル文書作成者装置１０２の概略構成を示した図である。

【００３７】

オリジナル文書作成者装置１０２は、CPU２０１と、CPU２０１のワークエリアとして機能するRAM２０２と、ハードディスク装置などの外部記憶装置２０３と、CD-ROMやFDなどの可搬性を有する記憶媒体２０５からデータを読取る読取り装置２０４と、キーボードやマウスなどの入力装置２０６と、ディスプレイなどの表示装置２０７と、ネットワークを介して他の装置と通信を行うための通信装置２０８と、上述した各構成要素間のデータ送受を司るインターフェイス２０９を備えた、一般的な構成を有する電子計算機２１０で構築することができる。

【００３８】

オリジナル文書作成者装置１０２の外部記憶装置２０３に格納されるのは、オリジナル文書作成PG（プログラム）２２１と署名生成PG（プログラム）２２２と文書保管要求PG（プログラム）２２３である。これらのプログラムは、RAM２０２上にロードされ、CPU２０１により、それぞれオリジナル文書作成処理部２４１、署名生成処理部２４２、文書保管要求処理部２４３というプロセスとして具現化される。そのほか、これらの各処理部の入出力となるデータ（オリジナル文書１０６、署名つきオリジナル文書１０７、署名用秘密鍵２１１）などが格納される。なお、署名用秘密鍵２１１はセキュリティの観点から特に厳重な管理が求められる。そのため、他のデータが格納された外部記憶装置とは異なる耐タンパ性のある装置内に格納してもよい。

【００３９】

文書管理装置１０３、開示文書作成者装置１０４、受信者装置１０５も、オリジナル文書作成者装置１０２と同様の構成を備える。ただし、文書管理装置１０３の外部記憶装置には、文書保管PG（プログラム）２２４と、開示対象文書送信PG（プログラム）２２５が格納され、また保管を要求された署名つきオリジナル文書が格納される。また、開示文書作成者装置１０４の外部記憶装置には、情報公開請求受付PG（プログラム）２２６、開示対象文書検索PG（プログラム）２２７、開示対象文書要求PG（プログラム）２２８、開示箇所決定PG（プログラム）２２９、開示文書作成PG（プログラム）２３０、開示文書公開PG（プログラム）２３１が格納される。また、受信者装置１０５の外部記憶装置には、情報公開請求PG（プログラム）２３２、開示文書検証PG（プログラム）２３３が格納される。

【００４０】

なお、以下の各形態の説明では、各プログラムは、あらかじめ、外部記憶装置２０３に格納されているものとしたが、必要なときに、FD、CDROMなどの他の記憶媒体または通信

媒体であるインターネットなどのネットワークまたはネットワークを伝搬する搬送波を介して、上記外部インターフェイスを介して外部記憶装置２０３またはRAM２０２に導入されてもよい。

【００４１】

図３は、以下の各形態において、オリジナル文書である行政文書を作成し、文書管理装置に保管するときの概要を示したフロー図である。なお、オリジナル文書を作成し保管する段階においては、将来的に情報公開請求を受けたときに、文書管理装置に保管された文書のうち、どの部分が公開されるべき情報であり、どの部分が公開されるべきでない情報であるかを、決定できるとは限らない。一般には、決定できないことが多いと考えられる。なお、各ステップ中の括弧内に、当該ステップの処理を行うプログラム名を示す。

オリジナル文書作成・保管フロー：（オリジナル文書作成者装置１０２の処理）

３０１：はじめ

３０２：オリジナル文書を作成（オリジナル文書作成PG２２１）

３０３：作成したオリジナル文書に対し署名を生成（署名生成PG２２２）

３０４：署名つきオリジナル文書を文書管理装置１０３に送信し登録を要求（文書保管要求PG２２３）（文書管理装置１０３の処理）

３０５：受信した署名付きオリジナル文書を登録（文書保管PG２２４）

３０６：おわり

図４は、以下の各形態において、一般市民からの情報公開請求を受けて、情報公開されるときの概要を示したフロー図である。なお、各ステップ中の括弧内に、当該ステップの処理を行うプログラム名を示す。

情報公開フロー：（受信者装置１０５の処理）

４０１：はじめ

４０２：開示文書作成者装置１０４に対し、情報公開を要求するために、公開を希望する情報の範囲を特定可能な情報を送信（情報公開請求PG２３２）（開示文書作成者装置１０４の処理）

４０３：公開を希望する情報の範囲を特定する情報を受信し（情報公開請求受付PG２２６）、その範囲を特定する情報に基づき開示すべき文書を検索し（開示対象文書検索PG２２７）、文書管理装置１０３に当該文書を要求（開示対象文書要求PG２２８）（文書管理装置１０３の処理）

４０４：要求された開示すべき署名つきオリジナル文書を開示文書作成装置１０４に送信（開示対象文書送信PG２２５）（開示文書作成者装置１０４の処理）

４０５：受信した署名つきオリジナル文書の内容を、あらかじめ定められた情報開示ポリシに照らして確認し、開示適当な箇所を決定し（開示箇所決定PG２２９）、個人情報や国家機密にかかわる情報などの開示不適当な情報が漏洩しないようにするための非開示処理を施した開示文書を作成し（開示文書作成PG２３０）、当該開示文書を受信者装置１０５に送信（開示文書公開PG２３１）（受信者装置１０５の処理）

４０６：受信した開示文書の真正性を検証（開示文書検証PG２３３）

４０７：おわり

以上に概要を示した情報公開システムにおいて、特に注意すべきなのは、開示文書の真正性の保証と、開示不適当な情報の削除の両立である。

【００４２】

開示文書がオリジナル文書と必ず同一であるような運用形態であれば、オリジナル文書作成者が、公知の電子署名技術を適用し、オリジナル文書にあらかじめ署名を付与しておけば、受信者は、開示文書（この場合はオリジナル文書と同一データ）の真正性を、公知の電子署名検証技術を適用することによって確認可能である。

【００４３】

しかし、本実施形態で述べるような情報公開システムにおいては、オリジナル文書と、開示文書が同一とは限らない。なぜなら、オリジナル文書には、情報公開時点では、開示することが不適当な情報（例：個人のプライバシーにかかわる情報、国家安全保障上公開

すべきでない情報など）が含まれている可能性があるため、これらの情報は非開示にされ、開示文書からは取り除かれる（i.e.墨塗りされる）必要があるからである。この場合の墨塗りのような情報公開の観点からは、適切あるいは必須と考えられるオリジナル文書に対する変更であっても、公知の電子署名技術では、悪意をもった第三者による改ざんを受けた場合と同様に、「検証できない」という結果しか得られない。

【００４４】

したがって、開示文書の真正性の保証と、開示不適当な情報の削除の両立可能な、新たな電子文書の真正性保証技術が求められる。

【００４５】

本実施形態における電子文書の真正性保証技術に望まれる性質は、以下の通りである。

（性質１）開示文書に非開示部分が含まれていても検証が可能であり、非開示部分以外に改変がなければ検証に成功すること。

（性質２）開示文書にオリジナル文書に対する墨塗り以外の改変があったときには検証が失敗すること。

（性質３）開示文書から非開示部分に関する情報が推定できないこと。

（性質４）開示文書の非開示部分の情報を推定しようとする攻撃者にとって、開示文書がその推定結果の正当性を保証する情報として利用できないこと。

【００４６】

上記の性質１は、公知の電子署名技術では達成できなかった点であるが、情報公開のようにオリジナル文書作成後になんらかの（適切な）変更が起こりうる場合には、必要となる要件である。

【００４７】

上記の性質２は、許される適切な改変（すなわち墨塗り）と、その他の改変を区別するための条件である。

【００４８】

上記の性質３は、非開示部分（墨塗り部分）から情報が漏洩しないことを意味する。たとえば、非開示部分の情報を暗号技術等によって隠して（暗号文として）公開する、という方法の場合には、当該暗号文が容易に解読されないように設計しなければならない。

【００４９】

上記の性質４は、たとえ非開示部分（墨塗り部分）が推定されたとしてもそれを否認できるようにすることを意味する。たとえば、オリジナル文書が「容疑者Ａは犯行を否認した」であり、開示文書が「容疑者＊＊＊＊は犯行を否認した」であったとする（すなわち開示文書作成者により個人情報であるＡの指名は非開示にされたとする）。この開示文書を見た攻撃者（受信者を含む）が、前後の文脈あるいは他の情報等から、「＊＊＊＊」は「Ａ」ではないかと推定し、＊＊＊＊部分にＡの氏名を仮に当てはめて検証を試みたとする。もし、この検証が成功したとすると、開示文書が、『「＊＊＊＊」は「Ａ」である』という推定結果を保証する情報として利用されるおそれがある。なぜなら「Ａ」以外の文字列で「＊＊＊＊」を当てはめたときに検証が成功する文字列が見出せる確率が事実上無視できる程度に小さくなる署名方法であったとすると、「Ａ」であることを否認するのは困難であるからである。

【００５０】

本実施形態においては、上記の各性質を満たす電子文書の真正性保証技術として適用しうる方法を複数開示する。

【００５１】

はじめに第１の実施形態について述べる。どのように実現するかを説明するために、オリジナル文書作成者装置１０２で動作する署名生成PG２２２と、開示文書作成者装置１０４で動作する開示文書作成PG２３０と、受信者装置１０５で動作する開示文書検証PG２３３の詳細について述べる。

【００５２】

図５は、第１の実施形態に従った署名生成PG２２２の処理フローを示した図である。

５０１：はじめ
５０２：オリジナル文書を構成要素（以降、ブロックと呼ぶ）に分割する。構成要素をどのように定めるかについては、たとえばオリジナル文書の先頭から１バイトごとにひとつの構成要素として定めてもよいし、あるいは、XML(eXtensible Markup Language)を使って記述された文書のようにあらかじめ構造化された文書であれば、その最小構成要素を利用してもよい。以下、オリジナル文書をＮブロックの列とみなす
５０３：オリジナル文書であるＮブロックの列の、すべての部分列に対し、それぞれオリジナル文書作成者の秘密鍵を用いて署名を生成する（２のＮ乗個の署名が生成されることになる）
５０４：オリジナル文書の部分列に対する２のＮ乗個の署名と、オリジナル文書とからなるデータを、署名付きオリジナル文書とする
５０５：おわり
図６は、第１の実施形態に従った開示文書作成PG２３０の処理フローを示した図である。
６０１：はじめ
６０２：開示対象である署名付きオリジナル文書の中から、開示不適切な情報を含むブロックを検索
６０３：検索されたブロック以外のブロックからなる、オリジナル文書の部分列を生成
６０４：前記部分列と、前記部分列に対応する署名とからなるデータを、開示文書とする
６０５：おわり
図７は、第１の実施形態に従った開示文書検証PG２３３の処理フローを示した図である。
７０１：はじめ
７０２：開示文書（オリジナル文書のある部分列と前記部分列に対応する署名とからなる）を、オリジナル文書作成者の公開鍵を用いて検証し、検証結果を出力する。なお、検証に利用するオリジナル文書作成者の公開鍵は、たとえば、開示文書とともに開示文書作成者装置１０４から送られてくるようにしてもよいし、オリジナル文書作成者装置１０２から、必要に応じて入手可能であるようにしておいてもよい。公開鍵は、公知のPKI(Public-key infrastructure)技術を適用して発行された、確かにオリジナル文書作成者であることを確認可能な公開鍵証明書つきで利用可能であることが望ましい
７０３：おわり
以上に述べた電子文書の真正性保証技術（第１の実施形態）が、上記の（性質１）（性質２）（性質３）（性質４）を満たしていることを説明する。

【００５３】

第１の実施形態では、開示文書は、オリジナル文書の部分列と、その部分列に対するオリジナル文書作成者の署名とから構成される。したがって、従来の電子署名の検証技術を適用することによって、開示文書の真正性を確認可能である。したがって、（性質１）（性質２）を満たす。また、開示文書には、開示不適当な情報を含むブロックは含まれない。したがって（性質３）を満たす。さらに開示文書に付された署名情報は、開示不適当な情報を含むブロックとは無関係である、すなわち、開示文書に付された署名を生成するときに、開示不適当な情報を含むブロックは入力情報として利用されていないため（性質４）も満たす。

【００５４】

以上に述べたように、第１の実施形態は、本実施形態において望まれる性質を満たすが、効率性の観点からみると課題がある。第１の実施形態では、Ｎブロックからなるオリジナル文書に対し、２のＮ乗個の署名を生成する必要がある。したがって、より効率のよい方法が望まれる。

【００５５】

次に、効率を改善した第２の実施形態について述べる。どのように実現するかを説明するために、オリジナル文書作成者装置１０２で動作する署名生成PG２２２と、開示文書作

成者装置１０４で動作する開示文書作成PG２３０と、受信者装置１０５で動作する開示文書検証PG２３３の詳細について述べる。

【００５６】

図８は、第２の実施形態に従った署名生成PG２２２の処理フローを示した図である。

８０１：ステップ５０２と同様

８０２：各ブロックのデータと当該ブロックがオリジナル文書中のどこに位置するかを示す位置情報とを結合したデータ（これを位置情報つきブロックと呼ぶ）に対し、署名を生成（Ｎ個の署名を生成）

８０３：各位置情報つきブロックのデータ（Ｎ個）と、各ブロックに対する署名（Ｎ個）とからなるデータを、署名付きオリジナル文書とする

８０４：おわり

なお、上記フローの中で、位置情報を結合しているのは、ブロックの順番を入れ替えるという不正行為を防止するためである。位置情報としては、たとえば当該ブロックが先頭から数えて何ブロック目であるかを示す連番を利用すればよい。もしブロックへの分割を先頭から１バイトずつ行っている場合には、この連番は、当該ブロックが先頭から何倍とめであるかをあらわすことになる。また、もしオリジナル文書が、XML(eXtensible Markup Language)などによって記述された構造化された文書である場合には、その構造を反映したより適切な情報を、位置情報として利用してもよい。

【００５７】

図９は、第２の実施形態に従った開示文書作成PG２３０の処理フローを示した図である。

９０１：はじめ

９０２：ステップ６０２と同様（ただし各ブロックは位置情報つきブロックとする）

９０３：検索されたブロック（i.e.非開示ブロック）以外の位置情報つきブロックと、前記各位置情報つきブロックに対応する署名（個数は開示ブロックの数に一致）とからなるデータを開示文書とする

９０４：おわり

図１０は、第２の実施形態に従った開示文書検証PG２３３の処理フローを示した図である。

１００１：はじめ

１００２：開示文書（ひとつまたは複数の位置情報つきブロックと各ブロックに対応する署名とからなる）を、オリジナル文書作成者の公開鍵を用いて、各ブロックごとに検証し、すべてのブロックの検証に成功したときに「検証成功」、それ以外のときに「検証失敗」と出力

１００３：おわり

以上に述べた電子文書の真正性保証技術（第２の実施形態）が、上記の（性質１）（性質２）（性質３）（性質４）を満たしていることを説明する。

【００５８】

第２の実施形態では、開示文書は、オリジナル文書の部分列と、その部分列を構成する各ブロックに対するオリジナル文書作成者の署名とから構成される。したがって、従来の電子署名の検証技術をブロックの数だけ繰り返し適用することで、開示文書の真正性を確認可能である。したがって、（性質１）（性質２）を満たす。また、開示文書には、開示不適当な情報を含むブロックは含まれない。したがって（性質３）を満たす。さらに開示文書に付された署名情報は、開示不適当な情報を含むブロックとは無関係である、すなわち、開示文書に付された署名を生成するときに、開示不適当な情報を含むブロックは入力情報として利用されていないため（性質４）も満たす。

【００５９】

以上に述べたように、第２の実施形態は、本実施形態において望まれる性質を満たす。また、効率性の観点からみても、第１の実施形態では、Ｎブロックからなるオリジナル文書に対し、２のＮ乗個の署名を生成する必要があったのに対し、第２の実施形態では、Ｎ

個の署名を生成すればよい。
【００６０】
次に、さらに効率を改善した第３の実施形態について述べる。なお後述するように第３の実施形態では、上記の（性質４）は満たさない。したがって、（性質４）を必要としないような情報公開システムに適用すべき方法である。どのように実現するかを説明するために、オリジナル文書作成者装置１０２で動作する署名生成PG２２２と、開示文書作成者装置１０４で動作する開示文書作成PG２３０と、受信者装置１０５で動作する開示文書検証PG２３３の詳細について述べる。
【００６１】
なお、第３の実施形態では、暗号学的ハッシュ関数（以下、単にハッシュ関数という）を利用する。本実施形態で利用するハッシュ関数とは、「任意長のデータを入力とし、固定長のデータを出力するような関数で、（１）出力からもとの入力を算出できない（一方向性）、（２）同じ出力を与える２つの入力を見つけることができない（衝突困難性）、という特徴を持つもの」である。具体的な例としては、たとえば、ＳＨＡ－１やＭＤ５として知られているものがある。
【００６２】
図１１は、第３の実施形態に従った署名生成PG２２２の処理フローを示した図である。
１１０１：はじめ
１１０２：ステップ５０２と同様
１１０３：各ブロックのデータのハッシュ値を算出し、算出されたＮ個のハッシュ値を結合したデータに対し、署名を生成（１個の署名を生成）
１１０４：ステップ１１０３で生成された署名（１個）と、オリジナル文書とからなるデータを署名付きオリジナル文書とする
図１２は、第３の実施形態に従った開示文書作成PG２３０の処理フローを示した図である。
１２０１：はじめ
１２０２：ステップ６０２と同様
１２０３：検索された各ブロックのハッシュ値と、それ以外の各ブロックと、署名とからなるデータを開示文書とする（i.e.検索された各ブロック（非開示ブロックに相当）についてはブロック自体ではなくハッシュ値を利用し、それ以外の各ブロック（開示ブロックに相当）についてはブロック自体を利用する）
１２０４：おわり
図１３は、第３の実施形態に従った開示文書検証PG２３３の処理フローを示した図である。
１３０１：はじめ
１３０２：開示文書（ひとつまたは複数のブロックのハッシュ値と、ひとつまたは複数のブロックと、署名とからなる）のうち、（ハッシュ値ではなく）もとのデータ自体が与えられている各ブロックのハッシュ値を算出する
１３０３：ステップ１３０２で算出された、または、開示文書に含まれるハッシュ値（合計Ｎ個）を結合したデータを、オリジナル文書作成者の公開鍵を用いて検証し、検証結果を出力する
１３０４：おわり
なお、第３の実施形態の場合にも、第２の実施形態と同様に、各ブロックの位置を特定する位置情報を利用してもよい。位置情報を利用した場合、ステップ１３０３でハッシュ値を結合する順番の決定が容易となる。
【００６３】
以上に述べた電子文書の真正性保証技術（第３の実施形態）が、上記の（性質１）（性質３）を満たし、（性質４）を満たさないことを説明する。
【００６４】
第３の実施形態では、開示文書は、オリジナル文書のうち開示可能なブロックに関する

ブロック自体と、開示不適当なブロックに関するブロックのハッシュ値と、オリジナル文書の各ブロックのハッシュ値を結合したデータに対するオリジナル文書作成者の署名とから構成される。したがって、受信者が、ブロック自体が開示されているブロックについてはそのハッシュ値を計算し、これらのハッシュ値と、ハッシュ値が開示されているブロックについての開示されたハッシュ値とを結合し、これを署名対象データとして署名検証すれば、開示文書の真正性を確認可能である。したがって、（性質１）を満たす。またハッシュ関数の衝突困難性により、オリジナル文書ブロックをハッシュ値ブロックに置き換える以外の変更は困難である。したがって（性質２）も満たす。また、開示文書に含まれる、開示不適当な情報に依存する情報は、開示不適当なブロックに関するブロックのハッシュ値と、そのハッシュ値に依存して生成された署名のみである。したがって、ハッシュ関数の一方向性により、（性質３）を満たすことがわかる。一方、前後の文脈等から開示不適当なブロックを推測した攻撃者は、推測が正しかったかどうかを、推測したブロックのハッシュ値を計算し、開示されたハッシュ値と一致するか否かを調べることで確認可能である。推測が正しかった場合、推定結果の正当性を保証する情報として利用されるため、第３の実施形態は、（性質４）を満たさない。

【００６５】

以上に述べたように、第３の実施形態は、上記望まれる性質のうち、（性質１）（性質３）は満たすものの、（性質４）は満たさない。しかし、効率の観点からは、Ｎブロックからなるオリジナル文書に対し、１個の署名を生成すればよいため、第２の実施形態よりも優れる。

【００６６】

次に、（性質４）を満たすように第３の実施形態を改良した第４の実施形態について説明する。オリジナル文書作成者装置１０２で動作する署名生成PG２２２と、開示文書作成者装置１０４で動作する開示文書作成PG２３０と、受信者装置１０５で動作する開示文書検証PG２３３の詳細について述べる。

【００６７】

図１４は、第４の実施形態に従った署名生成PG２２２の処理フローを示した図である。

１４０１：はじめ

１４０２：ステップ５０２と同様

１４０３：各ブロックに対し乱数を生成する（合計Ｎ個の乱数を生成する）

１４０４：Ｎ個のブロックそれぞれに対し、ブロックのデータとそのブロックに対して生成された乱数を結合したデータ（これを乱数つきブロックと呼ぶ）を生成する

１４０５：各乱数つきブロックのハッシュ値を算出し、算出されたＮ個のハッシュ値を結合したデータに対し、署名を生成（１個の署名を生成）

１４０６：ステップ１４０５で生成された署名（１個）と、Ｎ個の乱数つきブロックとからなるデータを署名付きオリジナル文書とする

１４０７：おわり

図１５は、第４の実施形態に従った開示文書作成PG２３０の処理フローを示した図である。

１５０１：はじめ

１５０２：ステップ６０２と同様（ただし各ブロックは乱数つきブロックとする）

１５０３：検索された各乱数つきブロックのハッシュ値と、それ以外の各乱数つきブロックと、署名とからなるデータを、開示文書とする（i.e.検索された各ブロック（非開示ブロックに相当）については乱数つきブロック自体ではなくハッシュ値を利用し、それ以外の各ブロック（開示ブロックに相当）については乱数つきブロック自体を利用する）

１５０４：おわり

図１６は、第４の実施形態に従った開示文書検証PG２３３の処理フローを示した図である。

１６０１：はじめ

１６０２：ステップ１３０２と同様（ただし各ブロックは乱数つきブロックとする）

１６０３：ステップ１３０３と同様
１６０４：おわり
なお、第４の実施形態の場合にも、第２の実施形態と同様に、各ブロックの位置を特定する位置情報を利用してもよい。位置情報を利用した場合、ステップ１６０３でハッシュ値を結合する順番の決定が容易となる。
【００６８】
以上に述べた電子文書の真正性保証技術（第４の実施形態）が、上記の（性質１）（性質３）（性質４）を満たすことを説明する。（性質１）（性質２）（性質３）については、第３の実施形態と同様である。以下、第４の実施形態が（性質４）を満たすことを説明する。第４の実施形態の場合は、前後の文脈等から開示不適当なブロックを推測した攻撃者が、推測が正しかったかどうかを、ハッシュ値を比較して調べることは困難である。なぜなら、仮に推測したブロックの情報が正しかったとしても、結合される乱数が正しくなければハッシュ値が一致しないからである。また、乱数は前後の文脈等とは無関係に生成されるため、乱数を推測することは著しく困難であり、事実上、不可能である。したがって第４の実施形態は（性質４）も満たす。
【００６９】
以上に述べたように、第４の実施形態は、上記望まれる性質を満たす。また、効率性の観点からみても、Ｎブロックからなるオリジナル文書に対し、第１の実施形態では、２のＮ乗個の署名を生成する必要があり、第２の実施形態では、Ｎ個の署名を生成する必要があったのに対し、第４の実施形態では、１個の署名を生成すればよく、優れている。
【００７０】
なお、上述の第４の実施形態の説明で用いた、ハッシュ関数の代りに、メッセージコミットメントスキーム(message commitment scheme)と呼ばれる関数を用いてもよい。メッセージコミットメントスキームとは、メッセージに対してcommitと呼ばれる値を計算する関数であって、
(Hiding)：commitから元のメッセージの情報を得ることが著しく困難である、
(Biding)：与えられたcommitと一致する元の入力メッセージと異なるメッセージを見つけることが著しく困難である、
という２つの性質を持つ関数のことである（元のメッセージが与えられたときに、それがcommitに対応していることを確認することは容易にできる）。メッセージコミットメントスキームの例は、たとえば、S.Halevi and S.Micali. ”Practical and Provably-Secure Commitment Schemes from Collision-Free Hashing”. In CRYPTO '96, LNCS 1109.Springer-Verlag, Berlin, 1996に開示されている。
【００７１】
上述の文献に開示されたメッセージコミットメントスキームは、ハッシュ関数を組み合わせて構成されているため、ハッシュ関数を単独で用いる場合に比べ、処理の負荷は大きいが、元のメッセージの情報が情報量的に秘匿されているという点では優れる。
【００７２】
図１７から図２０は、それぞれ第１から第４の実施形態に従って作成された、署名付きオリジナル文書１０７と開示文書１０８の構造の模式図（ブロック数が５で、第３ブロックが非開示ブロックの場合の例）である。
【００７３】
上記第２～４の実施形態にしたがって作成された開示文書では、追加的な墨塗りが可能である。すなわち、受信者や開示文書を入手した他のエンティティが、開示文書に含まれる開示文書作成者によって削除（墨塗り）されたブロック以外のブロックを、更に追加的に墨塗りすることができる。この性質は、利用場面によっては望ましくないと考えられることもある。
【００７４】
たとえば、図１に示した情報公開システムの場合に、開示文書作成者装置１０４から受信者装置１０５に対して送られる開示文書が、ネットワーク１０１上で、改変される恐れ

がある場合、不正者は開示文書に含まれる情報のうち不正者にとって都合の悪い情報を削除、すなわち追加的に墨塗りしたうえで、受信者装置１０５に送りつけることができる。この場合、受信者からみると、本来の開示文書と、不正者によって追加墨塗りされた開示文書とを区別できない（i.e.どちらもオリジナル文書の一部であることを確認できる）ため、情報公開の本来の目的からすると望ましいとはいえない。

【００７５】

そこで、電子文書の真正性保証技術に望まれる新たな性質として、

（性質５）開示文書に対する更なる墨塗りを防止可能であること、

を定義し、この性質も満たすように改良した第５の実施形態について述べる。

【００７６】

なお、本実施形態の説明においては、第４の実施形態で説明した電子文書の真正性保証技術をベースに構成した場合を例に挙げて説明するが、これに限定されず、他の真性性保証技術をベースに構成されてもよい。

【００７７】

第５の実施形態では、あらかじめ開示文書作成者装置１０４の外部記憶装置に、開示文書作成者の署名用秘密鍵が格納されているものとする。また、この署名用秘密鍵と対になる署名検証用の公開鍵は、たとえば、あらかじめWebサーバ上で受信者が入手できるものとする。なお、オリジナル文書作成者装置１０２における処理は基本的に第４の実施形態の場合と同様である。

【００７８】

第４の実施形態の説明中で図１５に示した開示文書作成PG２３０の処理フロー中のステップ１５０３を、以下のように変更する。

１５０３改：検索された各乱数つきブロックのハッシュ値と、それ以外の各乱数つきブロックと、署名とからなるデータに、開示文書作成者の署名用秘密鍵を用いて、開示文書作成者の署名を付与し、開示文書とする（i.e.第４の実施形態における開示文書に、開示文書作成者が署名を付与したものを、第５の実施形態における開示文書とする）

また第４の実施形態の説明中で図１６に示した開示文書検証PG２３３の処理フロー中のステップ１６０２を、以下のように変更する。

１６０２改：開示文書作成者の署名検証用の公開鍵を用いて開示文書に付された開示文書作成者の署名を検証する。検証が成功したときは、ステップ１３０２と同様（ただし各ブロックは乱数つきブロックとする）の処理を行う。検証が失敗したときは、開示文書は正当なものではないとみなし、終了する。

【００７９】

本実施形態によれば、開示文書作成者装置１０４において作成された開示文書に、開示文書作成者の署名が付与される。したがって、開示文書作成者以外のユーザによって、開示文書に対する追加墨塗りをされると、開示文書作成者の署名の検証に失敗するため、追加墨塗りを防止できる。

【００８０】

次に追加墨塗りに対する別の対策として、他の新たな性質として

（性質６）開示文書に対する更なる墨塗りを許容するか防止するかを開示文書作成者が選択可能であること、

を定義し、この性質も満たすように改良した第６の実施形態について述べる。

【００８１】

第５の実施形態では、開示文書全体に対する追加墨塗りを防止していたが、適用場面によっては、開示文書のうち、ある部分は追加墨塗りを防止したいが、別のある部分は追加墨塗りを許容したいというも考えられる。本実施形態によれば、このような追加的な墨塗りを許すか、あるいは、防止するかを、開示文書作成者が選択可能な、電子文書の真正性保証技術が提供される。

【００８２】

なお、第６の性質を満たせば、開示文書作成者が開示文書全他に対して、追加墨塗りを

防止するように設定することにより、開示文書に対する更なる墨塗りを防止可能となるため、第５の性質も満たす。

【００８３】

図２１は、第６の実施形態に従った、署名生成PG２２２の処理フローを示した図である。

２１０１：はじめ

２１０２：ステップ５０２と同様

２１０３：各ブロックに対し、乱数を生成する。これを「墨ブロック」と呼ぶ（合計Ｎ個の墨ブロックが生成される）

２１０４：ステップ１４０３と同様（ただしこのステップで生成される乱数は、ステップ２１０３で墨ブロックとして生成される乱数とは独立に生成されるものとする）

２１０５：ステップ１４０４と同様

２１０６：Ｎ個のブロックごとに、ステップ２１０５で生成された乱数つきブロックと、ステップ２１０３で生成された墨ブロックの２つのデータを、署名用２入力一方向性関数に入力し出力データを得る。その出力データ（Ｎ個）を結合したデータに対し、署名を生成する（１個の署名を生成）。ただし、ここで署名用２入力一方向性関数とは、以下を満たす関数でありシステム全体に知られているものとする。２つの値（Ａ，Ｂ）を入力とし、１つの値（Ｃ）を出力する関数であって、

（１）（Ａ'，Ｂ'）を入力したとき、Ａ'≠ＡかつＢ'≠Ｂならば無視できる確率を除いてＣ'≠ＣなるＣ'を出力する、

（２）ＡとＣを知っていても、無視できる確率を除いてＢを推定できない、

（３）ＢとＣを知っていても、無視できる確率を除いてＡを推定できない、

を満たすものとする。なお具体的な構成方法の例については後述する。

２１０７：ステップ２１０６で生成された署名（１個）と、Ｎ個の乱数つきブロックと、Ｎ個の墨ブロックからなるデータを署名つきオリジナル文書とする

２１０８：終わり

図２２は、第６の実施形態に従った、開示文書作成PG２３０の処理フローを示した図である。

２２０１：はじめ

２２０２：開示対象である署名付きオリジナル文書の中から、開示不適切な情報を含むブロックを検索

２２０３：検索されたブロック以外の各ブロックについて、「追加墨塗りを許容する」か「追加墨塗りを防止する」か、を決定

２２０４：開示不適切なブロックについては、墨ブロックを、開示しかつ追加墨塗りを防止するブロックについては、乱数つきブロックを、開示しかつ追加墨塗りを許容するブロックについては、墨ブロックと乱数つきブロックの両方を利用して構成されたデータと、署名とからなるデータを、開示文書とする

２２０５：おわり

図２３は、第６の実施形態に従った、開示文書検証PG２３３の処理フローを示した図である。

２３０１：はじめ

２３０２：開示文書（墨ブロックと乱数つきブロックと、署名とからなる）に含まれる各ブロックを署名用２入力一方向性関数に対応した検証用関数に入力し、出力を得る。検証用関数の具体的な構成方法の例については後述する。

２３０３：ステップ２３０２で算出された出力データ（Ｎ個）を結合したデータを、オリジナル文書作成者の公開鍵を用いて検証し、検証結果を出力する

２３０４：おわり

ここで説明した開示文書作成PG２３０にしたがって作成された開示文書を受け取った受信者は、開示文書作成者によって追加墨塗りを防止すると決定されたブロックについては、墨塗りすることができない。なぜなら、当該ブロックに対応する墨ブロックを入手でき

ないからである。

【００８４】

上述の署名用２入力一方向性関数と対応する検証用関数の具体的な構成例は以下の通りである。

（署名生成時）

入力値Ａ，Ｂに対し、２点（１，ｈ（Ａ）），（２，ｈ（Ｂ））を通る直線Ｌを求める（hはハッシュ関数）。次に直線Ｌ上のｘ座標が０，３の点（０，Ｑ），（３，Ｐ）を求め、Ｑ、Ｐを出力とする。なおＰは検証時に利用するため、補助データとしてステップ２１０７で開示文書に含めるものとする。

（署名検証時）

入力値Ａ'またはＢ'と、補助入力Ｐ'を入力とする。２点（１，ｈ（Ａ'））（または（２，ｈ（Ｂ'））と（３，Ｐ'）を通る直線Ｌを求める。次に直線Ｌ上のｘ座標が０の点（０，Ｑ'）を求め、Ｑ'Ｐ'を出力とする。

【００８５】

なお上述の構成において、ｘ座標の値０，１，２，３などはシステムに共通の値であればこれと異なっていてもよい。

【００８６】

署名用２入力一方向性関数と対応する検証用関数の別の構成例としては、次のように構成してもよい。

（署名生成時）

入力値Ａ，Ｂに対し、ｈ（Ａ），ｈ（Ｂ）を求め、これを結合したデータを出力とする（hはハッシュ関数）。なおｈ（Ａ），ｈ（Ｂ）は検証時に利用するため、補助データとしてステップ２１０７で開示文書に含めるものとする。

（署名検証時）

入力値Ａ'またはＢ'と、補助入力ｈ（Ａ）'，ｈ（Ｂ）'を入力とする。Ａ'が入力された場合には、ｈ（Ａ'）を計算し、これとｈ（Ｂ）'とを出力する。またＢ'が入力された場合には、ｈ（Ｂ'）を計算し、これとｈ（Ａ）'とを出力する。

【００８７】

本実施形態は、ネットワーク１０１に複数の開示文書作成者装置１０４が接続されていて、その間で文書が回覧されているような場合に特に効果的である。たとえば一つのオリジナル文書内に２つの領域AとBが存在し、領域A内の情報についての開示可否の判断を開示文書作成者Ｘが行い、領域Ｂ内の情報についての開示可否の判断を開示文書作成者Ｙが行うような運用をしたいとする。このとき、本実施形態に従うと、開示文書作成者Ｙが、領域Aの情報を（不当に）墨塗りを行う、といった本来の権限を越えた行為を防止可能である。

【００８８】

具体的には、まずオリジナル文書を受け取った開示文書作成者Ｘは、領域Ａ内の各ブロックについて開示の可否を判断し、開示する部分については、開示しかつ追加墨塗りを防止するブロックとして設定し、開示しない部分については墨塗りする。また領域Ｂ内の各ブロックについては、開示しかつ追加墨塗りを許容するブロックとして設定する。

【００８９】

このように設定された（ＸのＹに対する）開示文書を受け取った開示文書作成者Ｙは、領域Ｂ内の各ブロックについて開示の可否を判断し、開示する部分については、開示しかつ追加墨塗りを防止するブロックとして設定し、開示しない部分については墨塗りする。これを最終的な（受信者に対する）開示文書とする。このとき、領域Ａ内の各ブロックについては、追加墨塗りを防止するように設定されているため、開示文書作成者Ｙが、領域Aの情報を（不当に）墨塗りを行う、といった本来の権限を越えた行為を行うことはできない。

【００９０】

なお、先にオリジナル文書を受け取った開示文書作成者Ｘが、本来の権限を越えて、領

域Ｂ内の情報を墨塗りした場合には、開示文書作成者Ｙが、ＸのＹに対する開示文書を受け取った時にこの越権行為が判明するので、その時点で処理を中断する、あるいは開示文書作成者Ｘに再度開示文書作成処理をやり直させる、などの対策を行えばよい。

【００９１】

上記第１～６の実施形態では、情報公開制度を例に挙げて説明をしたが、本発明はこれに限定されるものではない。本発明が適用可能な別の一例として、PKI(Public-key Infrastructure)における公開鍵証明書の発行に本発明を適用した第７の実施形態について述べる。

【００９２】

図２４は、PKI(Public-key Infrastructure)における公開鍵証明書の構造を模式的に示した図である。

【００９３】

公開鍵証明書は、公開鍵の所有者を明らかにする目的で、一般に広く公開されうるデータであり、基本領域２４１０、拡張領域２４２０、認証局の署名２４３０から構成される。基本領域２４１０には、バージョン情報２４１１、シリアル番号２４１２、署名アルゴリズム２４１３、有効期間２４１４、発行者２４１５、所有者２４１６、公開鍵２４１７などの情報が含まれる。また拡張領域には、たとえば姓２４２１、名２４２２、生年月日２４２３、性別２４２４、住所２４２５、証明書ポリシに関する情報２４２６などが含まれる。

【００９４】

公開鍵証明書には、プライバシーにかかわる情報が含まれる可能性もある。たとえば図２３に示した公開鍵証明書の場合、拡張領域に含まれる、姓２４２１、名２４２２、生年月日２４２３、性別２４２４、住所２４２５はプライバシーにかかわる可能性のある情報である。このような情報が公開鍵証明書に含まれていることの利点としては、第三者に対してその情報（たとえば生年月日２４２３）が正しいことを説明できるという点が挙げられる。しかし、このような情報が公開鍵証明書に含まれている場合、逆にその情報（たとえば生年月日２４２３）を明かしたくないときにも、公開鍵の正当性を示すためには（すなわち認証局によって公開鍵証明書に付与された電子署名を確認するためには）、明かさざるを得なかった。

【００９５】

本発明を公開鍵証明書の発行に適用すると、生年月日を隠しつつ、公開鍵の正当性を示すことが可能になる。また、逆に生年月日が正しいことを説明したい場合には、生年月日を明かすことも可能である。

【００９６】

たとえば、拡張領域に含まれる各情報（姓２４２１、名２４２２、生年月日２４２３、性別２４２４、住所２４２５）を隠すことができるように公開鍵証明書を発行するためには、次のようにすればよい。

【００９７】

認証局が公開鍵証明書に対して署名を付与するときに、公開鍵証明書を、基本領域２４１０、姓２４２１、名２４２２、生年月日２４２３、性別２４２４、住所２４２５の６ブロックに分け、第１～６の各実施形態に示したいずれかの署名生成ＰＧの処理フローに従い、認証局の電子署名を生成する。この結果得られた、第１～６の各実施形態におけるオリジナル文書に相当するデータを公開鍵証明書とする。

【００９８】

発行された公開鍵証明書を入手した所有者は、たとえば生年月日を隠しつつ、公開鍵の正当性を示したい場合には、第１～６の各実施形態に示したいずれかの開示文書作成ＰＧの処理フローに従い、生年月日２４２３のブロックを墨塗りすればよい。

【００９９】

なお、公開鍵証明書に対して署名を付与する前に行う認証局の処理（例：本人性の確認など）や、署名付与後に行う認証局の処理（例：公開鍵証明書の配布など）については、

公知の認証局の処理と同様に行えばよい。

【０１００】

また、本発明を公開鍵証明書の発行に適用する別の形態として、複数の公開鍵に対応した単一の公開鍵証明書の発行への適用することも可能である。これを第８の実施形態として説明する。

【０１０１】

本実施形態によれば、複数の公開鍵に対する公開鍵証明書の発行を一度に行えるため、たとえば本人性の確認などの認証局が行う処理を一回で済ませることができ、効率的である。

【０１０２】

複数の公開鍵に対応した単一の公開鍵証明書の発行には次のようにすればよい。認証局が公開鍵証明書（ｎ個の公開鍵を含む）に対して署名を付与するときに、まず公開鍵証明書に公開鍵を記入する領域（公開鍵２４１７に相当）をｎ個設け、公開鍵証明書を、ｎ個の公開鍵の領域とその他の合計ｎ＋１個のブロックにわけ、第１～６の各実施形態に示したいずれかの署名生成ＰＧの処理フローに従い、認証局の電子署名を生成する。

【０１０３】

発行された公開鍵証明書を入手した所有者は、第１～６の各実施形態に示した開示文書作成ＰＧの処理フローに従い、たとえばｎ個の公開鍵のうちの第１番目以外を墨塗りすれば、第１～６の各実施形態における開示文書に相当するデータが、第１番目の公開鍵用の公開鍵証明書となる。

【０１０４】

公開鍵を更新したいとき（すなわち別の公開鍵を自分の公開鍵として使いたいとき）には、それまで使われたことのない公開鍵をひとつ選び、その他の公開鍵（それまでに使われていた公開鍵を含む）を墨塗りしすればよい。このとき、認証局に新たに公開鍵証明書を発行してもらう必要はない。

【０１０５】

なお、本実施形態の説明では、公開鍵証明書を、ｎ個の公開鍵の領域とその他の合計ｎ＋１個のブロックにわけていたが、これとは異なっていてもよい。たとえばその他の領域を細分化して複数のブロックに分けてもよい。さらには、第６の実施形態と組み合わせて適用してもよい。

【０１０６】

以上に述べた各実施形態では、電子署名技術をベースとして電子文書の真正性保証技術を構成した例を示したが、これと異なっていてもよい。たとえば、信頼できる第三者機関が存在する場合には、電子署名技術によらず、オリジナル文書作成者が、あらかじめ当該第三者機関装置にオリジナル文書（またはそのハッシュ値など）を預託しておき、受信者が当該第三者機関装置に開示文書の真正性を問い合わせるようにしてもよい。この場合であっても、本実施形態の説明で述べた第１～４の実施形態は適用可能である。たとえば、各方法で署名対象としたデータ（すなわち署名つきオリジナル文書のうちの署名以外のデータ）を、第三者機関装置に預託するようにすればよい。

【０１０７】

また、以上に述べた各実施形態では、主としてオリジナル文書が、構成要素であるブロックがシーケンシャルに並んだ構成をとっている場合を例にとって説明したが、これとは異なる構成をとっていてもよい。たとえば、XML(eXtensible Markup Language)などの構造化された文書フォーマットを使ってオリジナル文書が記述されている場合、各要素間に階層関係があると見ることができる。すなわち、Ａという要素名の開始タグと終了タグで囲まれた領域に、Ｂという要素名の開始タグ、終了タグが含まれている場合には、ＡはＢの親要素と見ることができる。このような階層構造がある場合には、その階層構造に応じて電子文書の真正性保証技術を設計してもよい。

【０１０８】

たとえば、第２の実施形態において、前述の説明では、各ブロックに対し、文書内にお

けるブロックの位置を示す位置情報として、連番を振るようにしていたが、これとは異なり、階層構造の中なかにおける位置を示す情報を利用してもよい。具体的には、たとえば階層構造をもつ一般的な文献において、文献内の位置を特定するときに用いられる「第Ｘ章、第Ｙ節、第Ｚ項」に相当する情報を、位置情報とすればよい（これに対し、一般的な文献におけるページ番号のように先頭から振られた連番を位置情報として利用した場合が、前述の第２の実施形態の説明に相当する）。あるいは、より一般に、適当な半順序(partial order)が定義された集合の元によって、位置情報を表現すればよい。

【０１０９】

また、本実施形態では、オリジナル文書を、互いに共通部分を持たない構成要素に分割して（ステップ５０２）署名生成を行う例を示したが、共通部分をもつ構成要素に分割してもよい。この場合であっても、本実施形態の説明で述べた第１～４の実施形態は適用可能である。

【０１１０】

なお、上記各実施形態では、非開示部分は墨塗り、すなわち、黒く塗りつぶした状態で開示する、と述べたが、このほかの方法により非開示処理を行っても良い。

【０１１１】

なお、上記各実施形態は行政文書を対象として説明したが、これに限定されるものではなく、署名付与後に署名対象部分の適切な改変が望まれることがあるさまざま電子文書に適用可能である。

【０１１２】

また、電子文書に限らず、より一般に、画像データ、動画データ、音楽データなどのディジタルデータに対しても適用可能である。この場合のブロックの設定は、それぞれのディジタルデータの構造に合わせて、適切に設定すればよい。

【図面の簡単な説明】

【０１１３】

【図１】実施形態を実現するネットワークシステムの概略構成図である。

【図２】実施形態におけるオリジナル文書作成者装置１０２を実現する計算機の概略構成図である。

【図３】実施形態におけるオリジナル文書作成・保管時のフローを説明する図である。

【図４】実施形態における情報公開時のフローを説明する図である。

【図５】第１の実施形態に従った署名生成PG２２２の処理フローを示した図である。

【図６】第１の実施形態に従った開示文書作成PG２３０の処理フローを示した図である。

【図７】第１の実施形態に従った開示文書検証PG２３３の処理フローを示した図である。

【図８】第２の実施形態に従った署名生成PG２２２の処理フローを示した図である。

【図９】第２の実施形態に従った開示文書作成PG２３０の処理フローを示した図である。

【図１０】第２の実施形態に従った開示文書検証PG２３３の処理フローを示した図である。

【図１１】第３の実施形態に従った署名生成PG２２２の処理フローを示した図である。

【図１２】第３の実施形態に従った開示文書作成PG２３０の処理フローを示した図である。

【図１３】第３の実施形態に従った開示文書検証PG２３３の処理フローを示した図である。

【図１４】第４の実施形態に従った署名生成PG２２２の処理フローを示した図である。

【図１５】第４の実施形態に従った開示文書作成PG２３０の処理フローを示した図である。

【図１６】第４の実施形態に従った開示文書検証PG２３３の処理フローを示した図である。

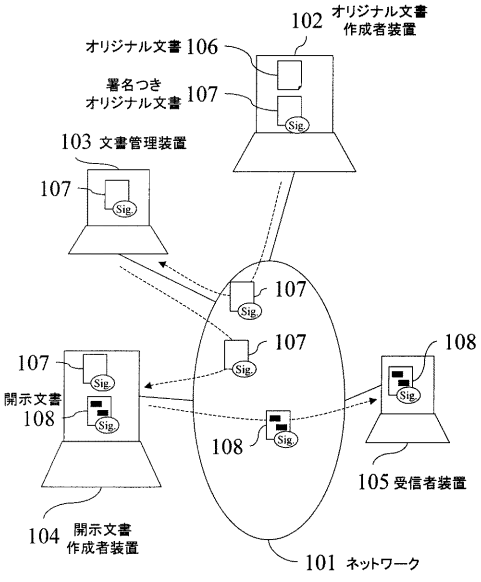
【図１７】第１の実施形態に従って作成された署名付きオリジナル文書１０７と開示文書１０８の構造の模式図である。

【図１８】第２の実施形態に従って作成された署名付きオリジナル文書１０７と開示文書

１０８の構造の模式図である。
【図１９】第３の実施形態に従って作成された署名付きオリジナル文書１０７と開示文書１０８の構造の模式図である。
【図２０】第４の実施形態に従って作成された署名付きオリジナル文書１０７と開示文書１０８の構造の模式図である。
【図２１】第６の実施形態に従った署名生成PG２２２の処理フローを示した図である。
【図２２】第６の実施形態に従った開示文書作成PG２３０の処理フローを示した図である。
【図２３】第６の実施形態に従った開示文書検証PG２３３の処理フローを示した図である。
【図２４】第７の実施形態における公開鍵証明書の構造を示した模式図である。
【符号の説明】
【０１１４】
１０１：ネットワーク、１０２：オリジナル文書作成者装置、１０３：文書管理装置、１０４：開示文書作成者装置、１０５：受信者装置、１０６：オリジナル文書、１０７：署名つきオリジナル文書、１０８：開示文書。

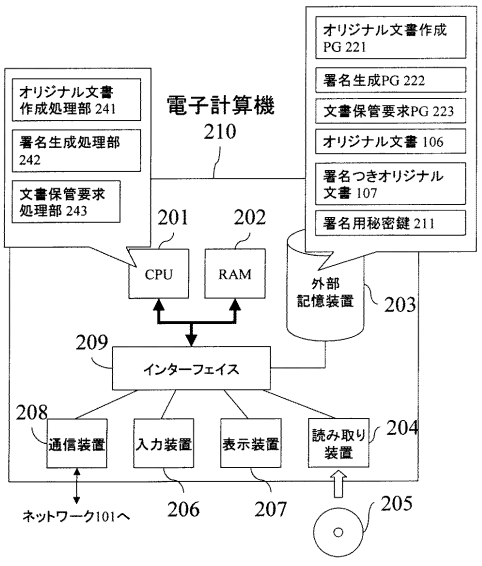
【図１】

図1



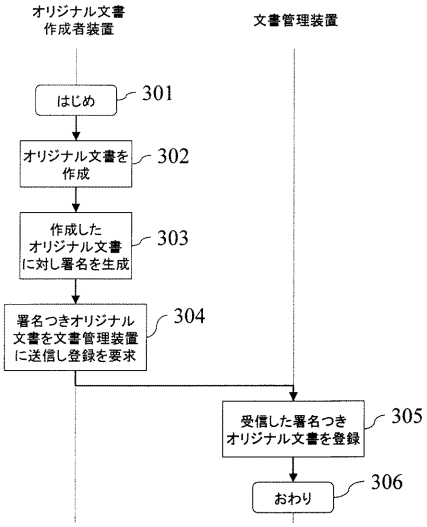
【図２】

図2



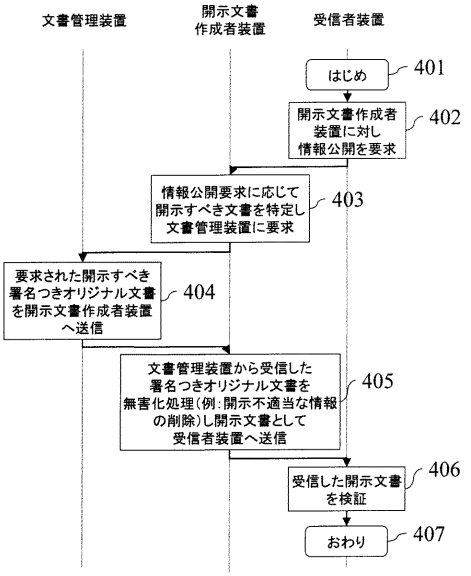
【図３】

図3



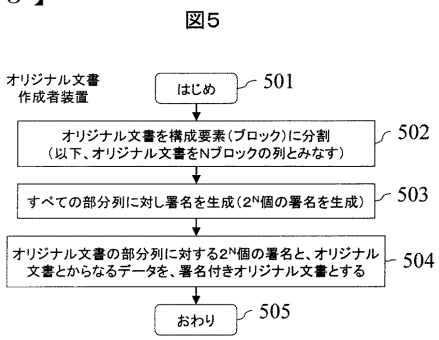
【図４】

図4



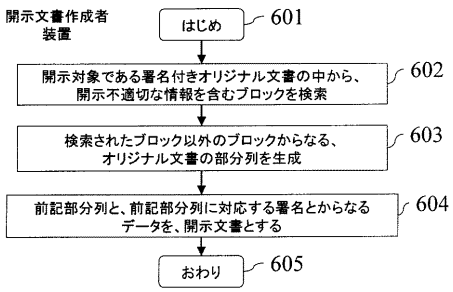
【図５】

図5



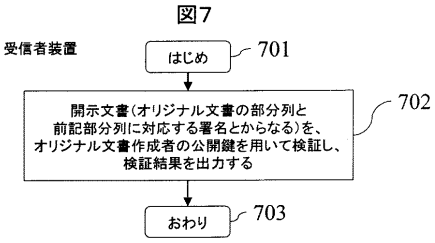
【図６】

図6



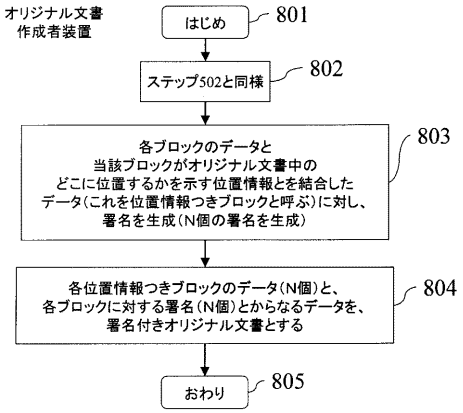
【図７】

図7



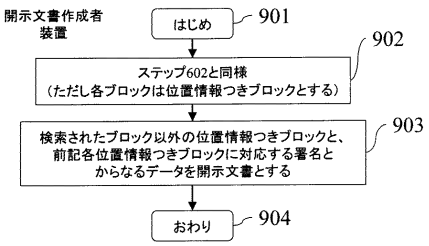
【図８】

図8



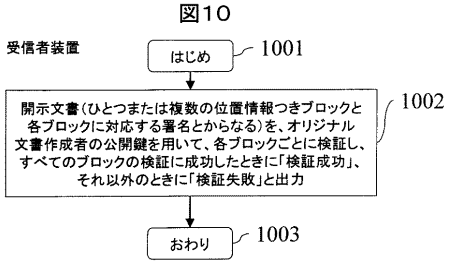
【図９】

図9



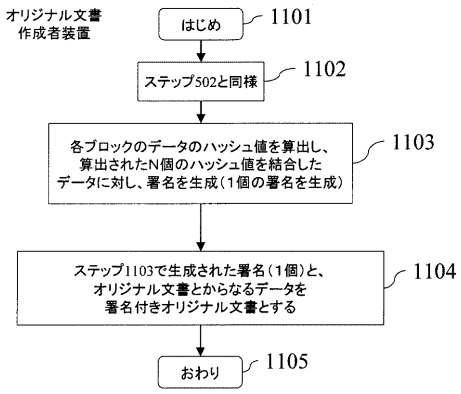
【図１０】

図10



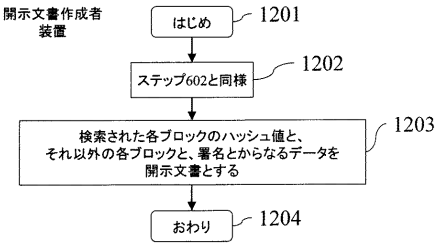
【図１１】

図11



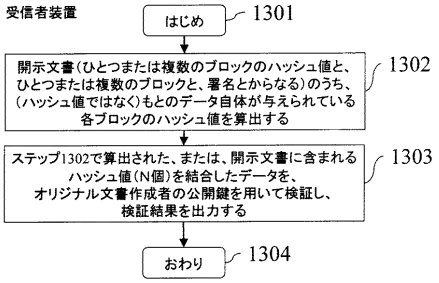
【図１２】

図12



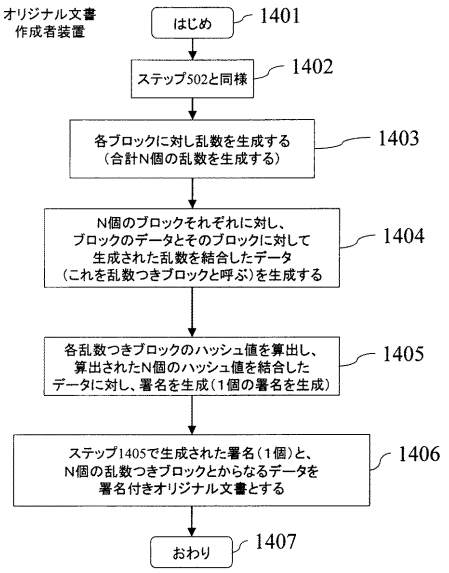
【図１３】

図13



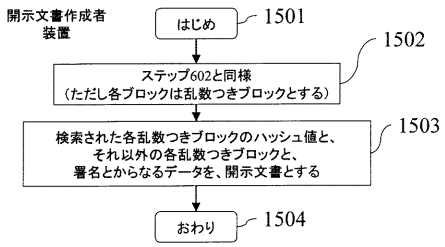
【図１４】

図14



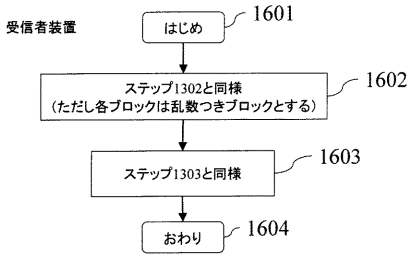
【図１５】

図15



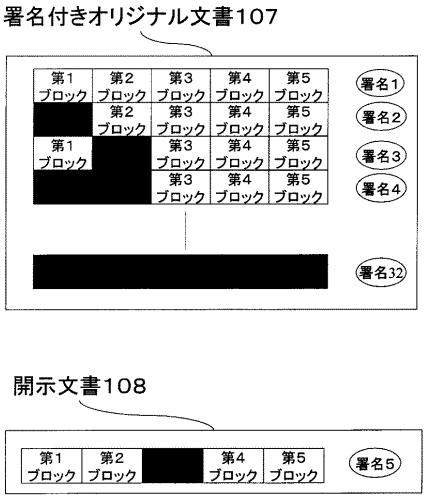
【図１６】

図16



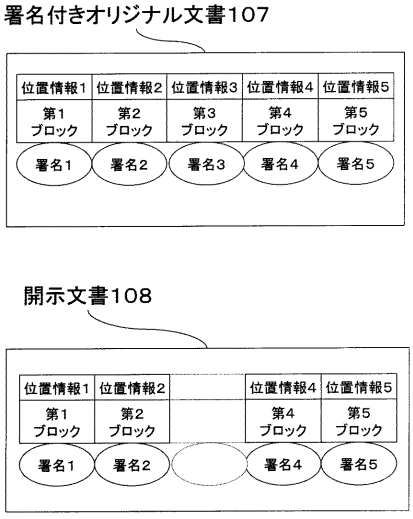
【図１７】

図17



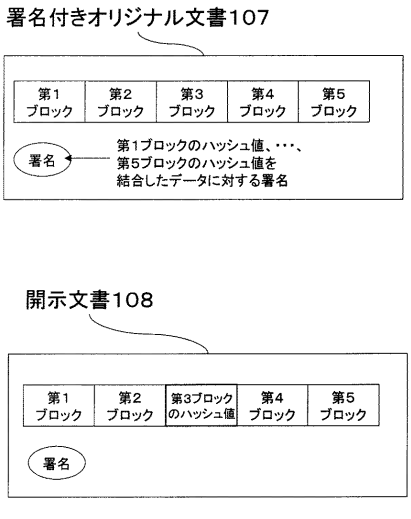
【図１８】

図18



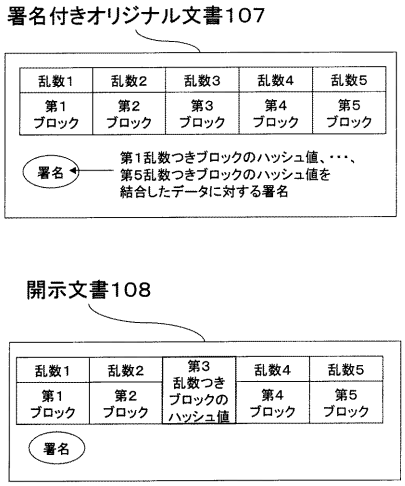
【図１９】

図19



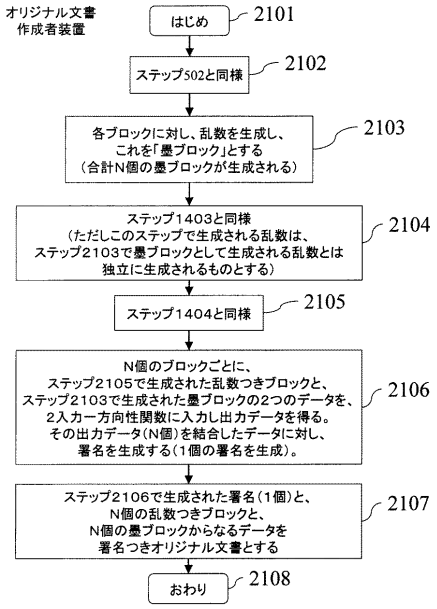
【図２０】

図20



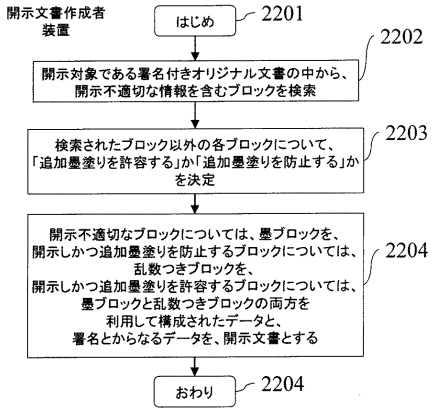
【図２１】

図21



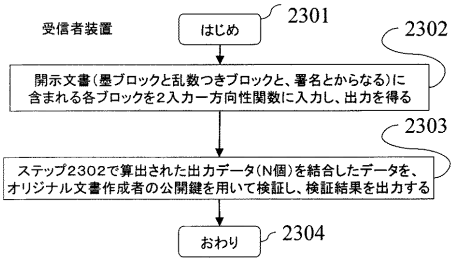
【図２２】

図22



【図２３】

図23



【図２４】

図24

フロントページの続き

(72)発明者　佐々木　良一
神奈川県藤沢市下土棚３２６－７
(72)発明者　吉浦　裕
東京都文京区本郷６－１９－７－２０１
(72)発明者　青島　弘和
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
(72)発明者　野山　英郎
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
(72)発明者　洲崎　誠一
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
(72)発明者　松木　武
神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所情報・通信グループＩＤソリューション統括本部内

Ｆターム(参考) 5B017 AA08　CA16
5J104 AA09　LA03